Department of the Army
Pamphlet 73–1

Test and Evaluation

Test and Evaluation in Support of Systems Acquisition

Headquarters
Department of the Army
Washington, DC
30 May 2003

UNCLASSIFIED

SUMMARY of CHANGE

DA PAM 73–1
Test and Evaluation in Support of Systems Acquisition

This administrative revision, dated 25 July 2024—

- Changes proponency from the Deputy Under Secretary of the Army to the Assistant Secretary of the Army (Acquisition, Logistics and Technology) (title page).

This Army pamphlet implements the policies contained in Army Regulation 73–1. Specifically it—

- Consolidates seven Department of the Army pamphlets: DA Pamphlet 73–1, 73–2, 73–3, 73–4, 73–5, 73–6, and 73–7.

- Provides an overview of the test and evaluation process in support of Army systems acquisition (chap 1).

- Describes the test and evaluation working-level integrated product team (chap 2).

- Provides detailed guidance and procedures for the preparation, staffing, and approval of the test and evaluation master plan (chap 3).

- Provides an overview of the Army critical operational issues and criteria development and approval processes (chap 4).

- Provides an overview of the Army system evaluation and system assessment process (chap 5).

- Provides an overview of Army developmental and operational testing processes (chap 6).

Headquarters
Department of the Army
Washington, DC
30 May 2003

*Department of the Army Pamphlet 73–1

Test and Evaluation

Test and Evaluation in Support of Systems Acquisition

By Order of the Secretary of the Army:

ERIC K. SHINSEKI
General, United States Army
Chief of Staff

Official:

JOEL B. HUDSON
Administrative Assistant to the Secretary of the Army

History. This publication is an administrative revision. The portions affected by this administrative revision are listed in the summary of change.

Summary. This pamphlet provides guidance and procedures to implement test and evaluation policy for materiel and information technology systems as promulgated by AR 73–1. It outlines the basic Army test and evaluation philosophy; general test and evaluation guidance in support of materiel systems acquisition and information technology systems acquisition; test and evaluation guidance in support of system modifications and nondevelopmental items; the test and evaluation working-level integrated product team; preparation, staffing and approval of the test and evaluation master plan; detailed guidance on preparation, staffing, and approval of critical operational issues and criteria, to include key performance parameters; guidance on the planning, conduct, and reporting of system evaluation; and guidance on the planning, conduct, and reporting of testing (that is, developmental and operational), to include test support packages, test incidents, corrective actions, instrumentation, targets, and threat simulators.

Applicability. The provisions of this pamphlet apply to the Active Army, the Army National Guard of the United States, and the U.S. Army Reserve. This pamphlet is not applicable during mobilization.

Proponent and exception authority. The proponent of this pamphlet is the Assistant Secretary of the Army (Acquisition, Logistics and Technology). The proponent has the authority to approve exceptions to this pamphlet that are consistent with controlling law and regulation. The proponent may delegate this approval authority, in writing, to a division chief within the proponent agency who holds the grade of colonel or the civilian equivalent.

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) via email to usarmy.pentagon.hqda-asa-alt.mbx.asa-alt-publication-updates@army.mil.

Distribution. This publication is available in electronic media only and is intended for command levels A, B, C, D, and E for the Active Army, the Army National Guard of the United States, and the U.S. Army Reserve.

Contents (Listed by paragraph and page number)

Chapter 1
Introduction, *page 1*
Purpose • 1–1, *page 1*
References • 1–2, *page 1*
Explanation of abbreviations and terms • 1–3, *page 1*
Test and evaluation roles and responsibilities • 1–4, *page 1*
Overview of test and evaluation support • 1–5, *page 1*
Basic test and evaluation elements • 1–6, *page 3*

Chapter 2
Test and Evaluation Working-Level Integrated Product Team, *page 5*
Integrated product team • 2–1, *page 5*
Test and evaluation working-level integrated product team overview • 2–2, *page 6*
Test and evaluation working-level integrated product team membership • 2–3, *page 7*
Test and evaluation working-level integrated product team charter • 2–4, *page 8*
Essential role of the test and evaluation working-level integrated product team • 2–5, *page 8*
Test and evaluation working-level integrated product team meetings • 2–6, *page 9*
Test and evaluation working-level integrated product team document review • 2–7, *page 10*

*This pamphlet supersedes DA Pamphlet 73–1, dated 28 February 1997; DA Pamphlet 73–2, dated 11 October 1996; DA Pamphlet 73–3, dated 1 March 1996; DA Pamphlet 73–4, dated 1 March 1997; DA Pamphlet 73–5, dated 30 September 1997; DA Pamphlet 73–6, dated 30 September 1996, and DA Pamphlet 73–7, dated 25 July 1997.

UNCLASSIFIED

Other test and evaluation working-level integrated product team considerations • 2–8, *page 11*

Chapter 3
Test and Evaluation Master Plan, *page 15*
Test and evaluation master plan procedures • 3–1, *page 15*
Test and evaluation master plan considerations • 3–2, *page 16*
Test and evaluation master plan requirements • 3–3, *page 16*
Principal test and evaluation master plan responsibilities • 3–4, *page 18*
Test and evaluation master plan review and approval process • 3–5, *page 20*
Test and evaluation master plan format and content • 3–6, *page 25*

Chapter 4
Critical Operational Issues and Criteria, *page 28*
Critical operational issues and criteria overview • 4–1, *page 28*
Critical operational issues and criteria relationships • 4–2, *page 30*
Development and approval processes for critical operational issues and criteria • 4–3, *page 35*
Critical operational issues and criteria–operational requirements document–test and evaluation master plan schedule synchronization • 4–4, *page 37*
Critical operational issues and criteria approval guidelines and staffing considerations • 4–5, *page 37*
Critical operational issues and criteria update considerations • 4–6, *page 39*
Critical operational issues and criteria checklist • 4–7, *page 39*
Critical operational issues and criteria development example • 4–8, *page 39*
Critical operational issues and criteria procedures for joint and multi-Service programs • 4–9, *page 39*

Chapter 5
System Evaluation, *page 40*

Section I
Introduction, page 40
Overview of system evaluation • 5–1, *page 40*
Scope of system evaluation • 5–2, *page 40*
Objectives of system evaluation • 5–3, *page 40*
System evaluation in support of systems acquisition and development • 5–4, *page 41*
System evaluation in support of other than new systems acquisition and development • 5–5, *page 45*

Section II
Requirements Translation, page 49
Overview of requirements • 5–6, *page 49*
Translating requirements • 5–7, *page 49*
Overview of the operational requirements document • 5–8, *page 50*
Development of evaluation issues • 5–9, *page 50*
Critical technical parameters • 5–10, *page 51*

Section III
System Evaluation Planning Process, page 51
System evaluation strategy overview • 5–11, *page 51*
Development of the system evaluation strategy • 5–12, *page 52*
Test and evaluation reviews • 5–13, *page 52*
Threat considerations in system evaluation • 5–14, *page 53*
System evaluation issues and criteria • 5–15, *page 55*
System evaluation tools • 5–16, *page 57*
Data sources for system evaluation • 5–17, *page 57*
Baseline correlation matrix • 5–18, *page 58*
Data source matrix • 5–19, *page 59*
Pattern of analysis • 5–20, *page 60*
Modeling and simulation • 5–21, *page 61*
Development of measures of effectiveness, measures of performance, and data requirements • 5–22, *page 64*

Section IV
System Evaluation Conduct, page 67
Development of the event design plan • 5–23, *page 67*
Analysis and evaluation of measures of effectiveness and measures of performance • 5–24, *page 67*

Section V
System Evaluation Reporting, page 68
System evaluation requirements • 5–25, *page 68*
System-level reports • 5–26, *page 68*
Event-level reports • 5–27, *page 69*
Source Selection Evaluation Board • 5–28, *page 69*

Chapter 6
Testing, *page 70*

Section I
Introduction, page 70
Overview of testing • 6–1, *page 70*
Philosophy of testing • 6–2, *page 70*
Waivers of approved testing • 6–3, *page 70*
Testing of commercial items and non-developmental items • 6–4, *page 70*
Testing of clothing and individual equipment • 6–5, *page 71*
Joint test and evaluation • 6–6, *page 71*
Multi-Service operational test and evaluation • 6–7, *page 72*
Testing in support of system changes • 6–8, *page 72*
Testing in support of reprocurements • 6–9, *page 72*
Foreign comparative testing • 6–10, *page 73*
Testing in support of limited procurement • 6–11, *page 73*
Testing in support of the combat and training development process • 6–12, *page 73*
Acquisition requirements package and Source Selection Evaluation Board • 6–13, *page 73*
Combined or integrated testing • 6–14, *page 73*

Section II
Developmental Testing, page 75
Overview of development testing • 6–15, *page 75*
Developmental test planning • 6–16, *page 76*
Developmental testing of non-tactical C4/IT systems • 6–17, *page 77*
Mission of the developmental tester • 6–18, *page 77*
Testing for commercial entities • 6–19, *page 77*
System contractor participation in developmental testing • 6–20, *page 77*
Developmental test data confirmation • 6–21, *page 78*
Developmental testing and the Army Logistician • 6–22, *page 79*
Developmental test types • 6–23, *page 79*
Requesting developmental test services • 6–24, *page 83*
Developmental test readiness review • 6–25, *page 84*
Developmental test readiness review working group • 6–26, *page 86*
Developmental test readiness review procedures • 6–27, *page 86*
Developmental test event design plan • 6–28, *page 90*
Developmental test incidents and related reports • 6–29, *page 91*
Developmental test detailed test plan • 6–30, *page 91*
Developmental test report • 6–31, *page 91*
Testing for climatic suitability and effectiveness • 6–32, *page 91*
Basic climatic design type • 6–33, *page 92*

Section III
Operational Testing, page 93
Overview of operational testing • 6–34, *page 93*

Operational test objectives in support of the materiel and tactical C4I/IT systems acquisition process • 6–35, *page 93*
Origin of operational test requirements • 6–36, *page 94*
Operational test types • 6–37, *page 94*
Operational testing of non-tactical C4/IT and space systems • 6–38, *page 95*
Operational test planning • 6–39, *page 95*
Operational test planning process • 6–40, *page 95*
Operational test event planning documentation • 6–41, *page 97*
Operational events • 6–42, *page 98*
Event design • 6–43, *page 98*
Entrance criteria for operational testing • 6–44, *page 102*
Operational test readiness review • 6–45, *page 103*
Operational test readiness statement requirements • 6–46, *page 104*
Safety release for operational testing • 6–47, *page 107*
Delay or termination of operational testing • 6–48, *page 108*
Operational test pretest activities • 6–49, *page 108*
Data authentication group operations • 6–50, *page 109*
System contractor relations • 6–51, *page 113*
Release of operational test information • 6–52, *page 113*
Operational test report • 6–53, *page 114*
Test data report • 6–54, *page 114*

Section IV
Test Support Packages, page 114
Test support packages overview • 6–55, *page 114*
Test support package applicability • 6–56, *page 115*
System support package • 6–57, *page 115*
New equipment training test support package • 6–58, *page 115*
Doctrinal and organizational test support package • 6–59, *page 116*
Threat test support package • 6–60, *page 120*
Training test support package • 6–61, *page 120*

Section V
System Safety Testing, page 125
Overview of system safety testing • 6–62, *page 125*
Safety and developmental testing • 6–63, *page 125*
Safety release • 6–64, *page 127*
Safety confirmation • 6–65, *page 128*

Section VI
Interoperability and Certification Testing, page 128
Overview of interoperability and certification testing • 6–66, *page 128*
Joint/Combined/North Atlantic Treaty Organization certification overview • 6–67, *page 128*
U.S. Army Communications-Electronics Command Software Engineering Center Army Participating Test Unit Coordinator's role in the Joint/Combined/North Atlantic Treaty Organization certification testing requirements • 6–68, *page 129*
North Atlantic Treaty Organization interoperability testing • 6–69, *page 129*
Tactical data links testing process • 6–70, *page 130*

Section VII
Instrumentation, Targets, and Threat Simulators, page 132
Instrumentation, targets, and threat simulators requirements • 6–71, *page 132*
Instrumentation, targets, and threat simulators planning • 6–72, *page 132*

Appendixes

A. References, *page 133*

B. Test and Evaluation Master Plan Checklist, *page 139*

C. Test and Evaluation Master Plan Approval Pages, *page 146*

D. Test and Evaluation Master Plan Format and Content, *page 153*

E. Critical Operational Issues and Criteria Format and Content, *page 164*

F. Critical Operational Issues and Criteria Process Guide, *page 176*

G. Critical Operational Issues and Criteria Checklist, *page 192*

H. Critical Operational Issues and Criteria Development Example, *page 195*

I. Survivability and Vulnerability Issue: System Evaluation Considerations, *page 201*

J. Live Fire Vulnerability/Lethality Issue: System Evaluation Considerations, *page 209*

K. Reliability, Availability, and Maintainability Issues: System Evaluation Considerations, *page 225*

L. Logistics Supportability (Including Transportability) Issue: System Evaluation Considerations, *page 229*

M. Manpower and Personnel Integration Issue: System Evaluation Considerations, *page 233*

N. System Safety Issue: System Evaluation Considerations, *page 234*

O. Interoperability Issue: System Evaluation Considerations, *page 238*

P. Natural Environmental Issue: System Evaluation Considerations, *page 240*

Q. Software Issue: System Evaluation Considerations, *page 241*

R. Department of Army Test Facilities, *page 310*

S. Live Fire Testing, *page 314*

T. Software Testing, *page 321*

U. Test and Evaluation Documentation Overview, *page 326*

V. Test Incident and Corrective Action Reporting, *page 338*

W. Survivability Testing, *page 366*

X. Operational Testing Entrance Criteria Templates, *page 376*

Y. Threat Considerations for Testing, *page 414*

Z. Instrumentation, Targets, and Threat Simulators, *page 421*

Table List

Table 3–1: Test and evaluation master plan preparation responsibility matrix, *page 19*
Table 4–1: Critical operational issues and criteria approval authorities, *page 37*
Table 5–1: Sample baseline correlation matrix, *page 58*
Table 5–2: Sample data source matrix, *page 60*
Table 5–3: Verification, validation, and accreditation responsibilities, *page 63*
Table 5–4: List of typical factors and conditions, *page 66*
Table 6–1: Basic climatic design type, *page 92*
Table 6–2: Environmental factors, *page 92*
Table 6–3: Operational testing entrance criteria matrix of templates, *page 102*
Table 6–4: Recommended operational test readiness review dates, *page 103*
Table 6–5: Levels of data, *page 111*
Table 6–6: Severity and joint task force impact, *page 131*
Table 6–7: Probability of occurrence, *page 131*
Table 6–8: Trouble report risk assessment, *page 132*
Table D–1: Measures of effectiveness and suitability, *page 154*

Table D–2: Critical technical parameters, *page 155*
Table D–3: Test and evaluation working-level integrated product team membership and roles, *page 157*
Table F–1: Planning factors for schedule synchronization, *page 182*
Table F–2: Schedule critical events, *page 183*
Table J–1: Comparison of joint live fire, Army live fire, and live fire test and evaluation programs required by Title 10, United States Code, *page 212*
Table J–2: Live fire test and evaluation event, *page 215*
Table J–3: Elements of firepower and survivability, *page 216*
Table J–4: Comparison of pre-shot modeling capabilities, *page 223*
Table N–1: Safety verification process—hazard probability categories (MIL–STD–882), *page 236*
Table Q–1: Areas of interest in Army software evaluation, *page 242*
Table Q–2: Software areas of interest and potential measures, *page 242*
Table Q–3: Metrics applicable to software fielding, *page 255*
Table Q–4: Software fielding decision criteria, *page 255*
Table Q–5: Metrics applicable to software transition, *page 258*
Table Q–6: Software transition decision criteria, *page 258*
Table Q–7: Army practical software and systems measurement common issues and software metrics, *page 259*
Table Q–8: Software metric—cost common issue—resources and cost, *page 261*
Table Q–9: Software metric—software engineering environment common issue—process performance, *page 263*
Table Q–10: Software metric—requirements traceability common issue—process performance, *page 266*
Table Q–11: Software metric—requirements stability common issue—product size and stability, *page 268*
Table Q–12: Software metric—design stability common issue—product size and stability, *page 270*
Table Q–13: Software metric—complexity common issue—product quality, *page 272*
Table Q–14: Software Metric—breadth of testing common issue—schedule and progress, *page 275*
Table Q–15: Software metric—depth of testing common issue—schedule and progress, *page 277*
Table Q–16: Software metric—fault profiles and common issue—schedule and progress, *page 279*
Table Q–17: Software metric—reliability common issue—product quality, *page 283*
Table Q–18: Software metric—manpower common issue—schedule and progress, *page 285*
Table Q–19: Software metric—development progress common issue—schedule and progress, *page 288*
Table Q–20: Software metric—schedule common issue—schedule and progress, *page 289*
Table Q–21: Software metric—computer resource utilization common issue—product quality, *page 291*
Table Q–22: Severity of risk event occurrence, *page 299*
Table Q–23: Likelihood of risk event occurrence, *page 299*
Table Q–24: Risk levels, *page 299*
Table Q–25: Example checklist of potential problems in implementing a software change package, *page 302*
Table Q–26: Determining the likelihood of a problem, *page 304*
Table Q–27: Determining the impact of a problem, *page 304*
Table Q–28: Checklists for integrated product team and configuration control board to address probability and impact of a problem, *page 304*
Table T–1: Metrics applicable to computer software configuration item qualification testing, *page 324*
Table T–2: Computer software configuration item qualification testing decision criteria, *page 324*
Table U–1: Test and evaluation documents, *page 326*
Table V–1: Header conventions for maintenance time, *page 352*
Table V–2: Header conventions for part information, *page 353*
Table X–1: Operational testing entrance criteria matrix of templates, *page 376*
Table Z–1: Validation report format and content, *page 430*
Table Z–2: Sample simulator/simulation validation report parametric data format, *page 436*
Table Z–3: Sample simulation summary report, *page 437*
Table Z–4: Threat simulator/simulation design system review and initial operational capability validation report, *page 438*
Table Z–5: Operational validation process, *page 439*

Figure List

Figure 1–1: Department of Defense 5000 systems acquisition model, *page 2*
Figure 2–1: Department of Defense integrated product team operational structure, *page 6*

Figure 2–2: Format of a test and evaluation working-level integrated product team charter, *page 14*
Figure 2–2: Format of a test and evaluation working-level integrated product team charter—Continued, *page 14*
Figure 3–1: Test and evaluation master plan development and test and evaluation working-level integrated product team coordination process, *page 21*
Figure 3–2: Test and evaluation master plan staffing for Office of the Secretary of Defense test and evaluation oversight programs, *page 21*
Figure 3–3: Test and evaluation master plan staffing for Missile Defense Agency programs, *page 22*
Figure 3–4: Test and evaluation master plan staffing for multi-Service Office of the Secretary of Defense test and evaluation oversight programs—Army lead, *page 23*
Figure 3–5: Test and evaluation master plan staffing for multi-Service Office of the Secretary of Defense test and evaluation oversight programs—Army Participant, *page 24*
Figure 3–6: Test and evaluation master plan staffing for non-Office of the Secretary of Defense test and evaluation oversight Acquisition Category II, Acquisition Category III, and Army special interest programs, *page 25*
Figure 3–7: Sample test and evaluation working-level integrated product team coordination sheet, *page 27*
Figure 3–7: Sample test and evaluation working-level integrated product team coordination sheet—Continued, *page 27*
Figure 4–1: Critical operational issues and criteria in the systems acquisition process, *page 29*
Figure 4–2: Critical operational issues and criteria relationships, *page 31*
Figure 4–3: Key performance parameter–critical operational issues and criteria relationship, *page 32*
Figure 4–4: Relationship of critical operational issues and criteria and performance exit criteria, *page 33*
Figure 4–5: Critical operational issues and criteria mission capability dendritic, *page 34*
Figure 4–6: System evaluation mission capability dendritic, *page 35*
Figure 4–7: Critical operational issues and criteria relationship to system evaluation measures, *page 36*
Figure 4–8: Critical operational issues and criteria process overview, *page 36*
Figure 4–9: Sample operational requirements document–critical operational issues and criteria crosswalk matrix, *page 38*
Figure 4–10: Time synchronization of operational requirements document, critical operational issues and criteria, and test and evaluation master plan, *page 38*
Figure 5–1: System change classification checklist, *page 47*
Figure 5–2: Models and simulation applications, *page 62*
Figure 5–3: Sample issue and criteria set, *page 65*
Figure 5–4: System-level reporting process decision, *page 68*
Figure 6–1: Joint/Combined/North Atlantic Treaty Organization interoperability testing cycle, *page 82*
Figure 6–2: Firm developmental test request, *page 85*
Figure 6–3: Considerations in preparation for the developmental test readiness review, *page 88*
Figure 6–3: Considerations in preparation for the developmental test readiness review—Continued, *page 88*
Figure 6–4: Sample developmental test readiness review agenda, *page 89*
Figure 6–5: Event planning process (repeated for each event), *page 97*
Figure 6–6: Pattern of analysis example format, *page 101*
Figure 6–7: Sample operational test readiness review agenda, *page 107*
Figure 6–7: Sample operational test readiness review agenda—Continued, *page 107*
Figure 6–8: Suggested format for a doctrinal and organizational test support package, *page 119*
Figure 6–8: Suggested format for a doctrinal and organizational test support package—Continued, *page 119*
Figure 6–9: Doctrinal and organizational test support package checklist, *page 122*
Figure 6–9: Doctrinal and organizational test support package checklist—Continued, *page 122*
Figure 6–10: Suggested format for a threat test support package, *page 122*
Figure 6–11: Training test support package checklist, *page 125*
Figure 6–11: Training test support package checklist—Continued, *page 125*
Figure 6–12: Initial areas of safety consideration, *page 125*
Figure 6–13: Minimum safety requirements done to provide data for the safety release, *page 127*
Figure 6–14: Checklist for North Atlantic Treaty Organization testing, *page 130*
Figure B–1: Test and evaluation master plan checklist, *page 145*
Figure B–1: Test and evaluation master plan checklist—Continued, *page 145*
Figure B–1: Test and evaluation master plan checklist—Continued, *page 145*
Figure B–1: Test and evaluation master plan checklist—Continued, *page 145*
Figure B–1: Test and evaluation master plan checklist—Continued, *page 145*

Figure B–1: Test and evaluation master plan checklist—Continued, *page 145*
Figure C–1: Test and evaluation master plan approval page for Office of the Secretary of Defense test and evaluation oversight programs, *page 147*
Figure C–2: Test and evaluation master plan approval page for Missile Defense Agency programs, *page 148*
Figure C–3: Test and evaluation master plan approval page for multi-Service Office of the Secretary of Defense test and evaluation oversight programs, *page 149*
Figure C–4: Test and evaluation master plan approval page for Acquisition Category II non-Office of the Secretary of Defense test and evaluation oversight programs, *page 150*
Figure C–5: Test and evaluation master plan approval page for multi-Service non-Office of the Secretary of Defense test and evaluation oversight Acquisition Category II programs, Army lead, and milestone decision authority is Army Acquisition Executive, *page 151*
Figure C–6: Test and evaluation master plan approval page for Acquisition Category III non-Office of the Secretary of Defense test and evaluation oversight programs, *page 152*
Figure D–1: Integrated test program summary, *page 156*
Figure D–2: Sample requirements/test crosswalk matrix, *page 163*
Figure E–1: Total operational system, *page 165*
Figure E–2: Critical operational issues and criteria structure, *page 166*
Figure E–3: Major elements of a criterion statement, *page 170*
Figure E–4: System versus organizational unit measure, *page 171*
Figure E–5: Characteristics of interest—mission accomplishment examples, *page 172*
Figure E–6: Characteristics of interest—sustainment examples, *page 173*
Figure F–1: Critical operational issues and criteria process for materiel and tactical C4I/IT programs, *page 177*
Figure F–2: Operational requirements document–critical operational issues and criteria crosswalk matrix, *page 179*
Figure F–3: Critical operational issues and criteria approval process for non-tactical C4/IT programs, *page 180*
Figure F–4: Materiel or tactical C4I/IT—combat developer proponent critical operational issues and criteria submission memorandum, *page 184*
Figure F–5: Materiel and tactical C4I/IT—major Army command headquarters critical operational issues and criteria position staffing memorandum, *page 185*
Figure F–6: Materiel and tactical C4I/IT—major Army command headquarters critical operational issues and criteria submission memorandum, *page 186*
Figure F–7: Materiel and tactical C4I/IT—Headquarters, Department of the Army (Deputy Chief of Staff, G–8) critical operational issues and criteria approval memorandum, *page 187*
Figure F–8: Non-tactical C4/IT—functional proponent critical operational issues and criteria submission memorandum, *page 188*
Figure F–9: Non-tactical C4/IT—major Army command headquarters critical operational issues and criteria position staffing memorandum, *page 189*
Figure F–10: Non-tactical C4/IT—major Army command critical operational issues and criteria submission memorandum, *page 190*
Figure F–11: Non-tactical C4/IT—Headquarters, Department of the Army (CIO/G–6) critical operational issues and criteria approval memorandum, *page 191*
Figure H–1: The situation, *page 197*
Figure H–1: The situation—Continued, *page 197*
Figure H–2: A solution, *page 200*
Figure H–2: A solution—Continued, *page 200*
Figure H–2: A solution—Continued, *page 200*
Figure J–1: Overview of the live fire test and evaluation process, *page 211*
Figure J–2: Live fire test and evaluation requirements flow chart, *page 213*
Figure J–3: Conceptual live fire test and evaluation approach to systems acquisition process, *page 215*
Figure Q–1: Cost and schedule performance, *page 262*
Figure Q–2: Cost indicator, *page 263*
Figure Q–3: Software engineering environment model indicator—continuous type, *page 265*
Figure Q–4: Software engineering environment model indicator—staged type, *page 266*
Figure Q–5: Software requirements traceability, *page 268*
Figure Q–6: Requirements stability—total requirements versus changes, *page 270*
Figure Q–7: Requirements stability—type of change, *page 270*
Figure Q–8: Design stability versus design progress graph, *page 272*

Figure Q–9: Software complexity—number of components, *page 274*
Figure Q–10: Software complexity—greater than threshold, *page 274*
Figure Q–11: Number of requirements tested, *page 276*
Figure Q–12: Requirements testing, *page 277*
Figure Q–13: Progress, *page 278*
Figure Q–14: Components successfully tested, *page 279*
Figure Q–15: Fault status, *page 282*
Figure Q–16: Fault aging, *page 282*
Figure Q–17: Mean-time-between-failure ranges, *page 284*
Figure Q–18: Reliability growth, *page 285*
Figure Q–19: Level of effort (plans vs actual), *page 287*
Figure Q–20: Staffing level planned vs actual, *page 287*
Figure Q–21: Staff experience, *page 288*
Figure Q–22: Design progress, *page 289*
Figure Q–23: Development milestone schedule, *page 291*
Figure Q–24: Milestone progress, *page 291*
Figure Q–25: Central processing unit utilization, *page 293*
Figure Q–26: Basic risk management process, *page 294*
Figure Q–27: Test and evaluation risk process methodology, *page 295*
Figure Q–28: Software fault profile metric example, *page 297*
Figure Q–29: Software faults by priority metric example, *page 298*
Figure Q–30: Typical information provided in a software problem change report, *page 306*
Figure Q–31: Problem change report category and criticality codes, *page 307*
Figure V–1: Sample DA Form 7492 (Test Incident Report), *page 340*
Figure V–1: Sample DA Form 7492 (Test Incident Report)—Continued, *page 340*
Figure V–2: Sample block 36 special requirements data, *page 341*
Figure V–3: Test incident data stream, *page 363*
Figure V–3: Test incident data stream—Continued, *page 363*
Figure V–3: Test incident data stream—Continued, *page 363*
Figure V–3: Test incident data stream—Continued, *page 363*
Figure V–3: Test incident data stream—Continued, *page 363*
Figure V–3: Test incident data stream—Continued, *page 363*
Figure V–3: Test incident data stream—Continued, *page 363*
Figure V–3: Test incident data stream—Continued, *page 363*
Figure V–4: Test incident report corrective action data stream, *page 365*
Figure V–4: Test incident report corrective action data stream—Continued, *page 365*
Figure X–1: Schedule operational testing entrance criteria template, *page 380*
Figure X–2: Requirements operational testing entrance criteria template, *page 382*
Figure X–2: Requirements operational testing entrance criteria template—Continued, *page 382*
Figure X–3: Analysis of alternatives OT entrance criteria template, *page 383*
Figure X–4: System threat assessment report OT entrance criteria template, *page 384*
Figure X–5: Maintenance concept OT entrance criteria template, *page 385*
Figure X–6: Concept of operations OT entrance criteria template, *page 386*
Figure X–7: TEMP OT entrance criteria template, *page 387*
Figure X–8: OT Event design plan entrance criteria template, *page 388*
Figure X–9: Deficiency identification and correction process OT entrance criteria template, *page 389*
Figure X–10: Security planning OT entrance criteria template, *page 390*
Figure X–11: Configuration management plan OT entrance criteria template, *page 391*
Figure X–12: Contractor testing OT entrance criteria template, *page 392*
Figure X–13: Developmental testing OT entrance criteria template, *page 393*
Figure X–14: Live fire testing OT entrance criteria template, *page 394*
Figure X–15: System performance OT entrance criteria template, *page 395*
Figure X–16: System maturity OT entrance criteria template, *page 396*
Figure X–17: Production representative articles OT entrance criteria template, *page 397*
Figure X–18: Interoperability and compatibility OT entrance criteria template, *page 398*
Figure X–19: Software development OT entrance criteria template, *page 399*

Figure X–20: Safety reviews and certifications OT entrance criteria template, *page 400*
Figure X–21: Deficiency resolution OT entrance criteria template, *page 401*
Figure X–22: Test team training OT entrance criteria template, *page 402*
Figure X–23: Personnel OT entrance criteria template, *page 403*
Figure X–24: T&E infrastructure OT entrance criteria template, *page 404*
Figure X–25: Modeling and simulation OT entrance criteria template, *page 405*
Figure X–26: Support equipment OT entrance criteria template, *page 406*
Figure X–27: Sufficiency of spares OT entrance criteria template, *page 407*
Figure X–28: Packaging, handling, and transportation OT entrance criteria template, *page 408*
Figure X–29: Support agreements and support contractors OT entrance criteria template, *page 409*
Figure X–30: Threat systems OT entrance criteria template, *page 410*
Figure X–31: Technical data OT entrance criteria template, *page 411*
Figure X–32: Central test support facility OT entrance criteria template, *page 412*
Figure X–33: Joint interoperability testing operational testing entrance criteria template, *page 413*
Figure Z–1: Project classification decision tree, *page 424*
Figure Z–2: Threat requirements generation process for targets and threat simulators, *page 427*
Figure Z–3: Validation/accreditation support to the Department of Defense life cycle model, *page 430*
Figure Z–4: Validation events in the life cycle of threat simulators/simulations, *page 434*
Figure Z–5: Validation working group membership pool, *page 435*
Figure Z–6: Validation event cycle, *page 436*
Figure Z–7: Army validation process for targets, *page 443*
Figure Z–8: Accreditation event cycle, *page 445*
Figure Z–9: Threat accreditation working group membership pool, *page 446*
Figure Z–10: Accreditation report letter of transmittal, *page 447*

Glossary

Chapter 1
Introduction

1–1. Purpose

The primary purpose of test and evaluation (T&E) is to support system development and acquisition by serving as a feedback mechanism in the iterative systems engineering process. This pamphlet provides guidance and procedures to implement T&E policy for materiel and information systems with regard to planning, executing, and reporting T&E in support of the acquisition process as promulgated by Army Regulation (AR) 73–1. Developing and deploying Army systems that are operationally effective, suitable, and survivable represents a significant challenge to all involved in the systems acquisition process. The procedures and guidelines in this pamphlet apply to—

a. All systems developed, acquired, and managed under the auspices of Department of Defense Directive (DoDD) 5000.01, Department of Defense Instruction (DoDI) 5000.02, and AR 70–1; these systems are referred to as materiel and command, control, communications, computers, and intelligence/information technology (C4I/IT); and AR 40–60; these systems are referred to as medical systems.

b. All systems managed and certified for interoperability under the auspices of DoDI 8330.01.

c. All special access programs under the auspices of AR 380–381.

d. Materiel developers (MATDEV), combat developers (CBTDEVs), functional proponents (FPs) for non-tactical C4I/IT systems, training developers (TNGDEVs), threat analysts, developmental testers, operational testers, system evaluators, Headquarters, Department of the Army (HQDA) staffers, and all others involved in the T&E of systems during acquisition. The term MATDEV when used in this pamphlet includes program, project, and product managers (PM) and their staffs unless otherwise stated. The term CBTDEV includes FPs unless otherwise stated.

1–2. References

Required and related publications and prescribed and referenced forms are listed in appendix A.

1–3. Explanation of abbreviations and terms

Abbreviations and special terms used in this pamphlet are explained in the glossary.

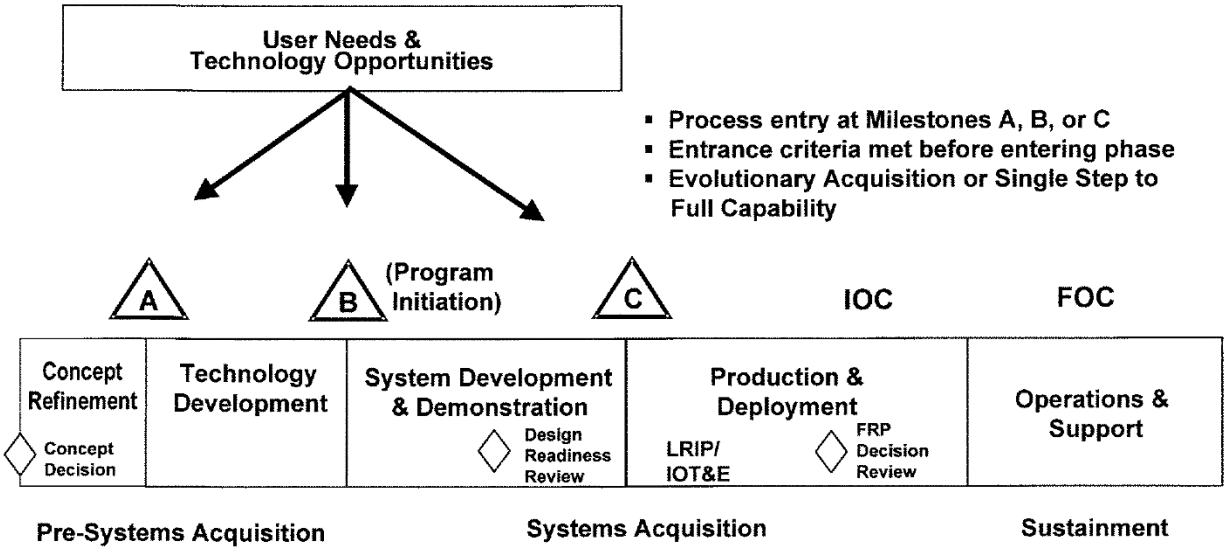
1–4. Test and evaluation roles and responsibilities

A fully coordinated and integrated T&E effort is essential for timely, effective, and efficient T&E. The Deputy Under Secretary of the Army (Operations Research) (DUSA (OR)), has oversight on all T&E policy and procedural issues for the Army. AR 73–1 provides the current T&E roles and responsibilities in support of acquisition of Army systems.

1–5. Overview of test and evaluation support

All acquisition programs are based on the identification of mission needs that only have a materiel solution. A mission needs analysis identifies the need for a new operational capability or improvement to an existing capability. One of the fundamental elements of the acquisition process is T&E. Figure 1–1 depicts the defense acquisition model in DoDI 5000.02.

a. The systems acquisition model is divided into three activities: Pre-systems acquisition, systems acquisition, and sustainment. Activities are divided into the following phases: technology development (Post Milestone A), system development and demonstration (Post Milestone B), production and deployment (Post Milestone C), and operations and support. A detailed description of the phases, milestones, and life-cycle activities for the acquisition life cycle model for all programs (that is, materiel and C4I/IT systems) is contained in DoDI 5000.02. Programs may enter the model at various points during pre-systems acquisition and systems acquisition. Under an evolutionary acquisition strategy, each subsequent increment beyond the first (that is, Increments 2 and 3), will follow the systems acquisition activities (that is, engineering and manufacturing development, demonstration, low-rate initial production (LRIP), and production). Army T&E has the flexibility to support any acquisition strategy appropriate for the acquisition program under consideration. The structuring and execution of an effective T&E program is absolutely essential to the development and deployment of Army systems that are operationally effective, suitable, and survivable while meeting the user's requirements.



FRP - Full-Rate Production
LRIP - Low-Rate Initial Production
IOT&E - Initial Operational Test and Evaluation

Figure 1–1. Department of Defense 5000 systems acquisition model

b. DoDD 5000.01 requires that T&E be closely integrated with requirements definition, threat projections, systems design and development, and support the user through assessments of a system's contribution to mission capabilities and support the defense acquisition process. T&E is the principal tool with which progress in system development is measured. The complexity of weapon systems, coupled with the need to reduce time and cost, demands that T&E programs be integrated throughout the acquisition process. Much of the information contained in independent evaluations and assessments is based on data generated from testing. It is Army policy that T&E programs be structured to integrate all developmental testing (DT), operational testing (OT), live fire testing (LFT), modeling and simulation (M&S), and other credible data generation activities appropriate to system evaluation. Integrated T&E serves as an efficient, integrated continuum that obtains necessary, authenticated data from many sources. This is accomplished to provide maximum benefit from a complete, unified T&E program by using resources efficiently to shorten acquisition time and determine whether systems are operationally effective, suitable, and survivable for their intended use. Both developmental and operational testers, in concert with the system evaluator, assist the MATDEV, CBTDEV, and TNGDEV in developing an integrated T&E strategy that optimizes the use of all testing, M&S, and other credible events as appropriate to the system.

c. The information generated as a result of T&E (for example, reports based upon test data, M&S data, and associated analyses) influences many of the actions taken during the system acquisition process and supports milestone decisions. Planning for T&E begins at the earliest stages of the system requirements, development, and acquisition processes. T&E can also reduce costs associated with upgrades, retrofits, and modernization by exposing problems that can be fixed prior to producing large numbers of items.

d. T&E provides information to—

(1) Decision makers responsible for procuring effective, suitable, and survivable systems.

(2) MATDEV for identifying and resolving technical and logistical issues.

(3) Managers for making the best use of limited resources.

(4) Operational users (for example, CBTDEV, trainers, and logisticians) for refining requirements and supporting development of effective doctrine, organization, training, and tactics, techniques, and procedures (TTP) for the system being acquired.

(5) The Joint Technical Coordinating Group for Munitions Effectiveness to aid in the development of Joint Munitions Effectiveness Manuals (JMEMs) used by operational forces and mission planners.

e. System contractors use T&E information to ensure compliance with contractually required specifications (for example, product definition data) and to detect manufacturing or quality deficiencies. System contractors often use test tools to ensure compatibility early in the development process to mitigate schedule slippages by early identification of problems.

f. Accredited models and simulations (M&S) are employed throughout the life cycle to support requirements definition; design and engineering; test planning, rehearsal, and conduct; result prediction; manufacturing; logistics support; training, and to include supplementing actual T&E. The Army has established verification, validation, and accreditation (VV&A) procedures for the use of M&S in support of T&E. DA Pam 5–11 contains these procedures. Computer-based M&S supports force-on-force; live fire; threat representation; synthetic, natural, and manmade environments; system operational and inter-operational loading (stimulation); and early examination of Soldier interface and mission capabilities, when live operations are either unsafe or resource prohibitive. In addition, force level M&S and/or Soldier in the loop virtual simulations may be used to extend live test findings to provide needed insight and data for system evaluation.

g. Army T&E policy provides the flexibility to allow each acquisition program to tailor a T&E strategy to achieve maximum support to the program. Hence, structuring a sound and efficient T&E program early in the system acquisition process is critical to the success of the program.

1–6. Basic test and evaluation elements

Army T&E consists of several basic elements that are essential in the development and conduct of meaningful T&E. These basic elements are—

a. Test and evaluation working-level integrated product team. The T&E working-level integrated product team (WIPT) is the cornerstone upon which a sound, effective T&E strategy is built and executed. The T&E WIPT assists the CBTDEV in the requirements generation process and MATDEV (or a PM, once established) in planning and managing the T&E throughout a system's life cycle. The primary objectives of the T&E WIPT are to provide for the basic planning for all life cycle T&E, identifying and resolving issues early, understanding the issues and the rationale for the approach, and assist the PM or MATDEV in producing a test and evaluation master plan (TEMP) that is acceptable to all organizational levels as quickly and as efficiently as possible. The T&E WIPT optimizes the use of appropriate T&E expertise, tools and instrumentation, facilities, simulations, and models to achieve T&E integration, thereby reducing costs to the Army and decreasing acquisition cycle time. A T&E WIPT will be established for every program, including special access programs, to ensure that T&E integration is accomplished. The T&E WIPT is composed of representatives from all organizations that have a role or may have a potential role in the T&E process and chaired by the PM or MATDEV. The T&E WIPT will also tailor the T&E tools and strategy to maximize effectiveness and efficiency. Details on organizational T&E players, rules, goals, and chartering of a T&E WIPT are discussed in chapter 2 of this pamphlet.

b. Test and evaluation planning documents.

(1) *Test and evaluation master plan.* The TEMP is the basic planning document for a system's life cycle that focuses on the overall structure, major elements, and objectives of the T&E program. The TEMP is the overarching T&E document for the many T&E planning, review, and reporting documents required of all acquisition programs. There is one TEMP for each acquisition system with the only exception being for investigational drugs, biologicals, and devices. A capstone TEMP is required for a program consisting of a collection of individual systems. The TEMP provides a road map for integrated simulation, T&E plans, schedules, and resource requirements necessary to accomplish the T&E program. The TEMP relates program schedule, test management strategy and structure, and required resources to critical operational issues and criteria (COIC); operational requirements document (ORD) requirements; critical technical parameters (CTPs); measures of effectiveness (MOEs) and measures of suitability (MOSs); and milestone decisions points. In order to ensure that a comprehensive system evaluation is conducted, the TEMP identifies and describes test events (that is, developmental, operational, and certification), M&S, and data collection (for example, baseline data from training exercises), as well as test resources, that are needed to satisfy key performance parameters (KPP), COIC, measures of performance (MOPs), MOEs, and MOSs from the system mission need statement (MNS) and ORD. Additionally, the organizations conducting the test events, M&S, and data collection are identified. The TEMP documents the T&E strategy and is initially developed for Milestone (MS) B. The TEMP is then updated before each MS and the Full-Rate Production (FRP) Decision Review (DR), when the program has changed significantly, when the program baseline has been breached, or when the associated ORD or command, control, communications, computers, and intelligence support plan (C4ISP) has been significantly modified. The TEMP is consistent with the acquisition strategy and the approved MNS, ORD, and C4ISP. Additionally, the TEMP is a reference document used by the T&E community to generate detailed T&E plans and to ascertain T&E schedule and resource requirements associated with a given system. An Army approved TEMP is required before commitment of T&E

resources. All T&E WIPT members contribute to the development and maintenance of the TEMP. The MATDEV (or PM) is responsible for the TEMP. Upon approval, the TEMP serves as a contract between the MATDEV, CBTDEV, and the T&E communities for executing the T&E strategy in support of the acquisition process to accommodate the unique characteristics and schedule of an acquisition program. Detailed TEMP procedures and format are in the Defense Acquisition Guidebook and chapter 3 of this pamphlet.

(2) *Critical operational issues and criteria.* COIC define the bottom line operational expectations of the system at the FRP DR. COIC reflect maturity expectations for the accomplishment of critical missions while considering the maturity of all doctrine, organizations, training, materiel, leadership and education, personnel, and facilities (DOTMLPF) components at that stage in the acquisition. COIC are the key decision maker operational concerns (issues) with standards of performance (criteria) that must be answered by the system evaluation to determine if the system is ready to enter FRP. COIC are the critical operational issues with associated scope, criteria, and rationale. COIC focus on mission accomplishment and reflect a just good enough system in the areas of training readiness, deployability, sustainability, and critical mission performance including survivability. A breach of a criterion is reason to delay entry into FRP unless other evidence of acceptable system operational effectiveness, suitability and survivability is provided. The criteria must relate to the ORD and the Analysis of Alternatives (AoA). Each ORD KPP will be a criterion. COIC are not usually separated into a set of categories such as effectiveness, suitability, and survivability. COIC by their very nature are overarching and will span such categories in a single issue or criterion. As appropriate, COIC will address the system-of-systems. COIC are initially developed and approved for the initial TEMP in support of MS B and are updated and approved for the MS C TEMP. Subsequent revisions of COIC occur for each increment under evolutionary acquisition and changes corresponding to a revised ORD. The approved COIC are included in the TEMP and are the basis for planning the system evaluation. Chapter 4 of this pamphlet discusses COIC in detail.

(3) *System evaluation plan.* The system evaluation plan (SEP) is the primary planning document for the independent system evaluation and assessment so as to ensure that only operationally effective, suitable, and survivable Army and multi-Service systems are delivered to the users. Critical to the decision making process is the availability of unbiased, objective evaluations and assessments of a system's capabilities. This is achieved by the use of evaluators who provide reports independent of the MATDEV and CBTDEV. System evaluation integrates experimentation, demonstration, and M&S information with available test data to address the evaluation issues (that is, CTPs, COIC and the additional issues (AIs) developed by the system evaluator). Through the SEP, the need for testing is determined and unnecessary testing avoided. The SEP documents the evaluation strategy and overall test/simulation execution strategy (T/SES) of a system for the entire acquisition cycle through fielding. The detailed information contained in the SEP supports concurrent development of the TEMP. The SEP is focused on evaluation of the system in the context of mission accomplishment, performance, safety, health hazard, and operational effectiveness, suitability, and survivability. The system evaluator, in coordination with the T&E WIPT, prepares the SEP. Per DoDI 5000.02, projects that undergo a Milestone A decision will have a T&E strategy that will primarily address M&S and early experimentation, including identifying and managing the associated risk, and strategy to evaluate system concepts against mission requirements. Chapter 5 of this pamphlet discusses system evaluation in detail.

(4) *Event design plan.* The event design plan (EDP) contains detailed information on event design, methodology, scenarios, instrumentation, simulation and stimulation, and all other requirements necessary to support the system evaluation requirements stated in the SEP. There will be one EDP for each primary data source identified in the SEP and TEMP. Chapters 5 and 6 of this pamphlet discuss system evaluation in detail.

c. Developmental testing and operational testing.

(1) The DT is an incremental continuum of tests, synchronized with product development, with a progression to a full-up system test. Ideally, DT events will provide the venue to fully demonstrate product performance and stability resulting in a system qualified for successful OT. DT can include gradual increased user participation. DT is performed in controlled environments, on the target hardware in an operational-like environment, and encompasses M&S and engineering type tests. Engineering tests are used to minimize design risks; determine physical and performance limits; provide software, security, system safety and interoperability certifications; determine compliance with system specifications; determine achievement of functional requirements and CTPs, and determine if the system is technically ready for OT and/or ready to enter the next acquisition phase. Per DoDI 5000.02, the MATDEV or PM must formally certify that the system is ready for OT.

(2) The OT is a field test of a system or item to examine its operational effectiveness, suitability, and survivability. OT is conducted under realistic operational conditions with users who represent those expected to operate and maintain the system when it is fielded or deployed. An initial operational test (IOT) is a special form of an OT, which is conducted using production or production representative units.

(3) A combined DT/OT approach is encouraged to shorten the acquisition process and reduce cost. The MATDEV, along with the T&E WIPT, must assess technical risks associated with choosing the combined DT/OT approach since the risk of an unsuccessful OT increases when insufficient technical performance and reliability data are available before OT. The combined DT/OT approach will not compromise either DT or OT test objectives or circumvent DT or OT entrance/exit criteria.

d. System assessment and continuous evaluation.

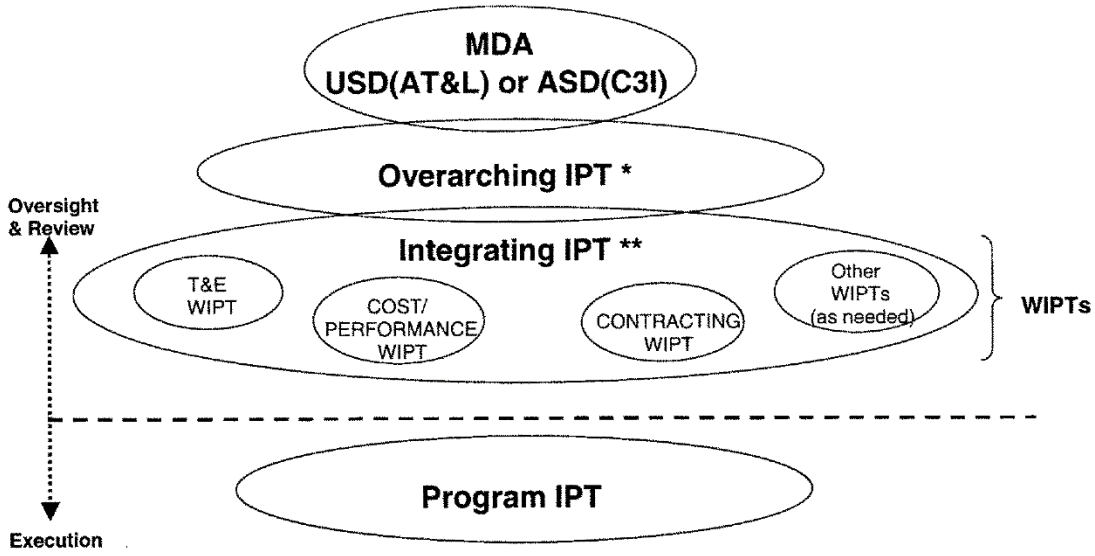
(1) *System assessment.* System assessment (SA) reports occur at key points during the system acquisition phases, before and after each milestone decision. As the system approaches a milestone or the FRP DR, the system evaluator will produce a system evaluation report (SER) to advise the DR principals and milestone decision authority (MDA) concerning the adequacy of testing, the system's operational effectiveness, suitability, and survivability, as well as recommendations for future T&E and system improvements. For a major defense acquisition program (MDAP), the system evaluation in support of the FRP DR will use data resulting from the IOT as a major data source integrated with other credible data sources as defined in the SEP. System evaluation focuses on demonstrated system technical and operational characteristics, performance, and safety as a part of system operational effectiveness, suitability, and survivability. SA examines a system's existing and potential capability so as to identify risks particularly when there is continuing development effort. Details on the planning, conduct, and reporting of system evaluation/assessment and continuous evaluation (CE) are in chapter 5 of this pamphlet.

(2) *Continuous evaluation.* CE is the process that provides a continuous flow of T&E information to all decision makers and developers on the progress towards a system achieving full operational capabilities. The process encourages frequent assessments of a system's status during development of the initial system as well as subsequent increment improvements and can result in a significant cost savings and reduce acquisition time through comparative analysis and data sharing. CE also examines whether a system is operationally effective, suitable, and survivable and satisfies the mission needs. CE is employed on all system acquisition programs. Upon request, system evaluators provide independent system evaluations and assessments to MATDEV or PM, CBTDEV, and TNGDEV. While in cooperation with the MATDEV, CBTDEV and other T&E WIPT members, the system evaluator must operate independently to ensure complete objectivity. CE is a strategy that ensures responsive, timely, and effective assessments of the status of an acquisition. CE should start as early as the requirements analysis for materiel systems and as early as the information management plan for non-tactical C4I/IT systems, and continue through post-deployment system support activities. CE provides unbiased, objective evaluations and assessments of a system's capabilities, flaws, benefits, burdens, and risks critical to the development and decision making processes. CE is important for T&E to support the acquisition process.

Chapter 2
Test and Evaluation Working-Level Integrated Product Team

2–1. Integrated product team

a. DoD has adopted integrated product teams (IPTs) as the preferred approach for the development, review, and oversight of the acquisition process. The IPT approach is to take advantage of all members' expertise, produce an acceptable product, and facilitate decision-making. PMs enhance the IPT process through establishing IPT plans of action and milestones (POA&M); proposing tailored documentation and milestone requirements; reviewing and providing early input to documents; resolving and elevating issues in a timely manner; and assuming responsibility to obtain principals' concurrence on issues, as well as with applicable documents or portions of documents. The POA&M provide a detailed understanding of key IPT activities, target dates, and deliverables. The POA&M is a management tool that complements the IPT Charter and communicates critical IPT objectives and the processes that will be used to achieve the overall system acquisition goals. Chartering an IPT, empowering qualified team members, training participants, aligning goals, open discussions, consistent team participation, resolving issues early, and preparing a POA&M provide a solid foundation to a successful and productive IPT. The "Rules of the Road: A Guide for Leading Successful Integrated Product Teams" provides guidelines for more effective IPT operations (available at https://www.dau.edu/cop/pm/documents/rules-road-guide-leading-successful-integrated-product-teams). Figure 2–1 depicts the overall DoD IPT structure.



* Required for ACAT ID and IAM

** For each program, there should be an Integrating IPT(IIPT)and at least one Working-level IPT (WIPT). An IIPT coordinates WIPT efforts and covers all topics not otherwise assigned to a WIPT. WIPTs focus on specific topics, for example, test and evaluation, cost/performance, and contracting.

Figure 2–1. Department of Defense integrated product team operational structure

b. At the Office of the Secretary of Defense (OSD) level, all acquisition category (ACAT) ID and IAM programs will have an overarching integrated product team (OIPT) to provide assistance, oversight, and review as the program proceeds through its acquisition life cycle. An appropriate official within OSD, typically the Director of Strategic and Tactical Systems or the Principal Director, Command, Control, Communications, Intelligence, Surveillance, and Reconnaissance and Space will lead the OIPT for ACAT ID programs. The Deputy DoD Chief Information Officer (CIO) or designee will lead the OIPT for ACAT IAM programs. The OIPT will consist of the PM, program executive officer (PEO), Component staff, Joint Staff, and OSD staff involved in the oversight and review of the particular ACAT ID or IAM program. A more detailed description of the operation of OIPT is in the Defense Acquisition Guidebook.

c. The PM or designee will form and chair an integrating integrated product team (IIPT) to support the development of strategies for acquisition and contracts, T&E, cost estimates, evaluation of alternatives, logistics management, and cost-performance trade-offs. An IIPT may be formed for all system acquisition programs. The PM or designee uses an IIPT to ensure that integration and coordination occur in order to properly address all aspects of the program's acquisition.

d. WIPTs are formed by the PM, or designee, through the IIPT process. The objective of a WIPT is to resolve as many issues and concerns at the lowest level possible, and to expeditiously escalate issues that need resolution at a higher level (that is, the Integrating IPT or OIPT), bringing only the highest level issues to the MDA for decision. Any unresolved issue should be addressed through the chain-of-command. In the Army, T&E policy and procedural issues will be brought forward through the Test and Evaluation Management Agency (TEMA) for DUSA (OR) adjudication.

e. WIPTs meet as required to help the PM plan program structure as well as document and resolve issues. WIPT can vary in size and serve as advisory bodies to the PM by assisting the PM in developing strategies and in program planning, as requested by the PM.

2–2. Test and evaluation working-level integrated product team overview

T&E integration is accomplished through the use of the T&E WIPT or the integrated test team if a T&E WIPT has not been established. The primary purpose of the T&E WIPT is to develop an integrated T&E strategy, as well as a coordinated program for M&S, developmental tests, and operational tests that will support a determination of whether or not a system is operationally effective, suitable, and survivable. The T&E WIPT operates within the IPT guidelines of the Defense Acquisition Guidebook, the Under Secretary of Defense (Acquisition, Technology and Logistics) (USD

(AT&L)) "Rules of the Road: A Guide for Leading Successful Integrated Product Teams," AR 70–1, and DA Pam 70–3. The T&E WIPT is a team of qualified, motivated, and innovative members representing their respective organizations. The T&E WIPT meets (or otherwise provides a forum) to plan the necessary testing and evaluation strategies, identify and resolve issues early, understand the issues and rationale for the approach, and to produce a coordinated TEMP prior to approval. The T&E WIPT members are members of the acquisition team. They are both knowledgeable and empowered to represent the interests of their organization and will remain as a principal working group member throughout the system acquisition process. The emphasis is on the word "team." As a team, it is extremely important that T&E WIPT members have defined roles, work interdependently while representing their functional area skills, and work in a trusting environment. Close coordination among the T&E WIPT members must be effected in a timely manner in order to optimize schedules and costs and preclude duplication or voids in the acquisition T&E cycle.

a. The T&E WIPT goals are to develop a mutually agreeable T&E program that will provide the necessary data for evaluations. T&E WIPTs provide support for the development, staffing, coordination, and approval of all required T&E documentation. T&E WIPTs establish the necessary subordinate working groups (for example, reliability, availability, and maintainability (RAM), LFT&E, and M&S subgroups) to develop a T&E strategy and address related T&E issues. T&E WIPTs ensure all participants have the opportunity to be involved. T&E WIPTs establish and manage the corrective action process; participate in the DT & OT test readiness reviews (TRRs); and support CE and integrated T&E. The use of T&E WIPTs optimizes the use of appropriate T&E expertise, instrumentation, targets, facilities, and M&S to achieve T&E integration, thereby reducing costs to the Army and decreases acquisition cycle time and mutually resolving cost and scheduling problems. T&E WIPT members must ensure that their actions do not cause unnecessary resource requirements, which is the primary cause of program funding and scheduling challenges for PMs. The PM should be supportive of T&E resource requests that are reasonable and justifiable. T&E WIPTs ensure T&E planning, execution, and reporting are directed towards a common goal. T&E WIPTs provide a forum in which designated representatives from the participating organization can discuss freely each person's views on the program and test requirements. Recommendations and documents will be products of the T&E WIPT.

b. Planning for T&E begins at the earliest stages of development of user needs, science and technology, system requirements, development, and acquisition processes. The MATDEV for materiel and tactical C4I/IT programs will form T&E WIPTs after approval of the DOTMLPF Needs Analysis Report stating and justifying the materiel need but not later than core staffing of the draft ORD. For other than ACAT I and information assurance (IA) programs, the DOTMLPF needs analysis report with a materiel need is equivalent to a MNS. For ACAT I or IA programs, the report justifies writing a MNS. For non-tactical C4I/IT programs, the MATDEV will form the T&E WIPT between the business process reengineering analysis and core staffing of the ORD (or ORD equivalent document if total program cost is less than $10 million). For programs with a Milestone A, the T&E WIPT must be established in time to develop, coordinate, and submit the T&E strategy to the approval authority. For programs without a MS A, a T&E WIPT needs to be established in sufficient time for the development, coordination, and approval of the initial TEMP in support of program initiation and the T&E portions of the request for proposal (RFP) and supporting documentation.

2–3. Test and evaluation working-level integrated product team membership

a. Organizations that have a role, or may have a potential role, in a program's T&E are extended invitations to the initial T&E WIPT meeting. Such organizations include but are not limited to the following—

(1) Principal members.

(a) MATDEV (PEO, PM, or other as appropriate).

(b) CBTDEV or FP for non-tactical command, control, communications, computers, and information technology (C4/IT).

(c) System evaluator.

(d) Developmental tester.

(e) Operational tester.

(f) Logistician (Assistant Secretary of the Army (Acquisition, Logistics and Technology) (ASA (ALT)) integrated logistics support (ILS) or designated representative).

(g) U.S. Army Research Laboratory (ARL), Survivability/Lethality Analysis Directorate (SLAD).

(h) TNGDEV or trainer.

(i) Threat integrator (TI) (Deputy Chief of Staff (DCS), G–2 or designated representative).

(j) User's or test unit's resource coordinators.

(k) Any command or agency that has a role critical to the success of the program (such as agencies that provide analysis, survivability, lethality, interoperability, nuclear, biological, chemical (NBC) survivability, safety, health hazard, manpower and personnel integration (MANPRINT), transportability, IT, or other considerations).

(2) For HQDA TEMP approval programs, the following HQDA offices are included: DUSA (OR); ASA (ALT); ASA (ALT) ILS; DCS, G–1; DCS, G–2; DCS, G–3; DCS, G–4; DCS, G–8; and the CIO/G–6. Failure of any of these offices to provide representatives to attend the initial T&E WIPT (or declare intent not to participate in the T&E WIPT process) forfeits organizational inclusion in the coordination of the TEMP prior to HQDA approval.

(3) For OSD level TEMP approval programs, representatives from Director, Operational Test and Evaluation (DOT&E) and the cognizant OIPT leader (that is, development test and evaluation (DT&E) or command, control, communications, computers, and intelligence (C4I)) may participate in the T&E WIPT.

b. System contractors may be invited to the T&E WIPT to provide information, advice, and recommendations; however, the following policy will govern their participation.

(1) System contractors will not be formal members of the T&E WIPT.

(2) System contractor participation will be consistent with Title 5, United States Code, Chapter 10 (5 USC Chapter 10).

(3) System contractors may not be present during T&E WIPT deliberations on acquisition strategy or competition sensitive matters, nor during any other discussions that would give them a marketing or competitive advantage.

c. Support contractors may participate in T&E WIPT meetings, but they may not commit the organization they support to a specific position. The organizations they support are responsible for ensuring the support contractors are employed in ways that do not create the potential for an organizational conflict of interest.

d. There are three T&E WIPT core members: MATDEV, CBTDEV, and system evaluator. T&E WIPT meetings should be scheduled to accommodate all core members. At the conclusion of the initial T&E WIPT meeting, those organizations that are essential to the success of the T&E WIPT will be identified. A T&E WIPT Charter will identify organizational representatives as either a principal or associate member.

2–4. Test and evaluation working-level integrated product team charter

The MATDEV or PM, regardless of ACAT level, will charter the T&E WIPT. The charter documents the mission and products of the T&E WIPT and establishes the timeframe in which the effort is to be completed. It establishes the membership, scope, objectives, and procedures of the T&E WIPT. A sample format is depicted at figure 2–2. The charter is finalized based on the initial T&E WIPT meeting and approved by the PM or MATDEV command only upon concurrence by the principal T&E WIPT members. See paragraph 2–3*a*(1) for a list of potential principal members. A copy of the approved charter is provided to each of the T&E WIPT members. While chaired by the PM or MATDEV, the T&E WIPT members will be composed of qualified T&E representatives empowered to speak and act on behalf of their organization.

2–5. Essential role of the test and evaluation working-level integrated product team

a. The T&E WIPT objectives are to identify and resolve issues early, understand the issues and the rationale for the approach, and document a quality TEMP that is acceptable at all organizational levels as quickly and as efficiently as possible. All documents should be delivered in a timely manner to keep pace with the system's T&E and acquisition schedules. The T&E WIPT will—

(1) Be established and chaired by the PM, MATDEV, or designated representative to assist with the development of the post-MS A T&E Strategy, if applicable, and the CTP, COIC, and TEMP in support of program initiation. To ensure an integrated effort, the T&E WIPT must coordinate with other WIPTs.

(2) Integrate T&E requirements and accelerate the TEMP coordination process by producing a coordinated TEMP, resolving cost and schedule problems, and determining test data requirements.

(3) Provide a forum to assist personnel responsible for T&E documentation and execution, and ensure that T&E planning, execution, and reporting are directed toward common goals. The T&E WIPT will be the forum through which T&E coordination among all members of the acquisition team, to include the system contractor, is accomplished. Minority opinions will be documented.

(4) Immediately elevate disagreement on matters of substance through the IIPT or command channels to the next higher level for resolution. Unresolved T&E issues will be brought through the proper chain-of-command to the DUSA (OR) for adjudication.

(5) Establish necessary subgroups to address related T&E issues and action items. Subgroup members will normally be responsible for those T&E issues and action items related to their particular functional area that are specified on an action item list (AIL). The AIL will be revised by organizational representatives at each subgroup meeting and become part of the minutes.

(6) Support the CE process by accomplishing early, more detailed, and continuing T&E documentation, planning, integration, and promote the sharing of data.

(7) Within their area of expertise, assist in preparing the T&E portions of the acquisition strategy, the RFP, and related contractual documents, and assist in evaluating contractor or developer proposals when there are T&E implications.

(8) Operate under the spirit and principles of the IPT and integrated product and process management or integrated product and process development (IPPD). The T&E WIPT will adhere to principles in the Defense Acquisition Guidebook to include open discussion, proactive participation, empowerment, and early identification and resolution of issues.

(9) Coordinate on requests for waivers of testing in an approved TEMP.

b. Minutes of all T&E WIPT meetings will be prepared by the T&E WIPT chairperson and distributed within 10 working days.

2–6. Test and evaluation working-level integrated product team meetings

T&E WIPT meetings encompass activities such as development and coordination of the TEMP to include resolution of issues whenever possible, coordination of applicable T&E documentation, establishment of necessary subgroups; managing the corrective action process; supporting the CE process; addressal of substantive T&E issues; briefings by special interest activities (for example, safety, environmental, software, and identification of problems and resolution of issues).

a. For programs with a MS A, the initial meeting should occur immediately following MS A, for the express purpose of developing, coordinating, and obtaining approval of the T&E strategy. For programs moving toward program initiation, the initial T&E WIPT meeting should be held in conjunction with the core staffing review of the draft ORD to familiarize the T&E WIPT members with the preliminary system requirements. The meeting will identify all principal T&E WIPT members, finalize the draft T&E WIPT Charter, and task T&E WIPT members to prepare input for the T&E strategy or initial TEMP, as applicable. For programs approaching program initiation (that is, MS B), this initial meeting may review a strawman TEMP (that is, a preliminary draft TEMP) produced jointly by the core T&E WIPT members (that is, MATDEV, CBTDEV, and system evaluator). The initial meeting can also be used to support the PM in developing the T&E strategy for incorporation into the draft acquisition strategy.

b. Notice of the initial T&E WIPT meeting should be sent at least 14 calendar days (preferably 30 calendar days) prior to the meeting. A draft agenda should accompany the notice. The agenda should be finalized with input solicited from the T&E WIPT members. The notice should also include a copy of the approved DOTMLPF Needs Analysis and, for an ACAT I or IA programs, the approved MNS. For programs preparing for program initiation, the notice should also include the draft ORD and, if available, a draft acquisition strategy.

c. The following actions should be accomplished at the initial T&E WIPT meeting—

(1) Provide a program or system orientation briefing, including a discussion of the draft system acquisition strategy. At the initial meeting, it is likely that attendees will be unfamiliar with the new program and it is necessary to familiarize them with all aspects of the program.

(2) Review available system requirements documents to familiarize members with preliminary system requirements. The CBTDEV should conduct the review. Describe the overall acquisition approaches that are being considered (or that will be employed), identifying areas needing the T&E community's input in the early planning of the acquisition strategy to ensure adequate T&E is integrated into the overall program.

(3) Initiate development of the T&E strategy for incorporation into the draft acquisition strategy.

(4) Initiate dialogue to define the CTPs to be addressed in T&E. Review the CBTDEV's plan and status of the COIC and KPP.

(5) Identify existing data, as well as M&S, test, and other data generation requirements for the respective life cycle phases that will support system development and generate data for the system evaluation required for each milestone.

(6) Task T&E WIPT members to draft their respective portions of the TEMP if a strawman is not provided. If a strawman was prepared, T&E WIPT members' comments and recommended changes should be discussed. Agreement should be reached on changes to be made, issues to be resolved, and the corresponding schedule leading to the T&E WIPT members signing the TEMP Coordination Sheet at a future T&E WIPT meeting (commonly referred to as the TEMP "Signing Party").

(7) Draft the T&E WIPT Charter. Ensure all T&E WIPT members (principal and associate) are identified. Define the roles and responsibilities of each T&E WIPT member organization, to include funding responsibilities.

(8) Review available contract documentation. Generally, contractual documentation has not been prepared at this point, however it is important to stress that a major function of the T&E WIPT members is to review contractual documents for T&E adequacy. If there is a draft statement of work (SOW) or RFP, it is useful to highlight the contractual requirements for T&E.

(9) Establish required subgroups.

(10) Discuss related document development and status, which affect T&E planning; related document completion is necessary to facilitate the T&E process (for example, COIC, the safety assessment report, the security classification guide, safety release (SR), environmental documentation, independent safety assessments, and system safety risk assessments (SSRAs)).

(11) Establish unique identifiers for the test title and system name for the purpose of initializing a database in the Army Test Incident Reporting System (ATIRS). Determine which tests require test incident reports (TIRs) (see para 6–29) and identify them in the TEMP.

(12) Record the minutes and action items. After the meeting the chairperson will prepare the meeting minutes including the AIL, and distribute as agreed to at the meeting and in the T&E WIPT Charter.

(13) Establish the distribution list for the T&E WIPT minutes containing all pertinent information (for example, actual name of each T&E WIPT member, organizational mailing address, phone and facsimile numbers, and email address).

(14) Discuss the action items assigned and develop a tentative agenda for the next meeting.

(15) Establish, as a minimum, the following ground rules whenever T&E WIPT industry participation exists:

(a) At the beginning of each meeting, the T&E WIPT chair will introduce each industry representative, including the representative's affiliation and purpose for attending.

(b) Chair will inform the T&E WIPT members of the need to restrict discussions while industry representatives are in the room, and/or the chair will request the industry representatives to leave before matters are discussed that are inappropriate for them to hear.

(16) Review training requirements and training development documents to ensure that training and train-up issues of the system evaluator and participants are identified early in the testing process. The TNGDEV should conduct the review.

d. Follow-on T&E WIPT meetings should occur on a timely basis to continue the T&E planning effort and the development, coordination, and approval of the required T&E documentation, especially the TEMP. The progress of the test program will be addressed and subgroups will meet as appropriate. As program changes occur and T&E details are developed, program planning modifications will be required. Discussion of issues should occur continuously and, upon resolution, closed out in the AIL. Ground rules associated with industry participation in the T&E WIPT process must be adhered to. The T&E WIPT members will participate in TRRs to coordinate and resolve T&E issues. Techniques for data collection, incident reporting, and other test peculiar issues should be fully coordinated and integrated within the T&E community. A T&E WIPT can be held at any time when it is necessary to assemble the many organizations involved in the T&E process for the program. Reasons for convening a T&E WIPT meeting include when the program is restructured; when an event presents a serious conflict for the next series of tests; during a test to disseminate information; or when a significant event or change to the program occurs.

2–7. Test and evaluation working-level integrated product team document review

T&E WIPT members will be afforded a timely opportunity to review and provide input on draft documents so as to ensure accurate T&E documentation. T&E WIPT concurrence is not sought during the T&E WIPT review. Document reviews may identify issues for the T&E WIPT to attempt resolution and, if not satisfactorily resolved to all concerned, elevated to the IIPT or proper chain of command channels. If necessary, the DUSA (OR) will adjudicate the issues. Typical documents reviewed by the T&E WIPT consist of—

a. Acquisition Strategy.
b. ORD.
c. C4ISP.
d. COIC.
e. AoA Study Plan or Report.
f. RFP and SOW.
g. System Specifications.
h. System Threat Assessment Report (STAR).
i. System Training Plan (STRAP).
j. SEP.
k. Test and M&S EDPs.
l. Outline test plans (OTPs).
m. Request for waivers.

2–8. Other test and evaluation working-level integrated product team considerations

Each of the following areas are considered during the T&E WIPT planning process and are discussed in detail in later chapters of this pamphlet.

a. Multi-Service acquisition programs with Army lead will have the same Army T&E WIPT membership as an Army unique acquisition program. Participating Services will determine their membership requirements to be documented in the T&E WIPT Charter. Multi-Service programs with Army participation (not Army lead) will have, as a minimum, representatives from the PM or MATDEV, CBTDEV or FP, system evaluator, and the DUSA (OR). If any Army unique testing is planned, the appropriate test agency will also be represented. As in all cases, membership is documented in the T&E WIPT Charter. T&E WIPT participation and TEMP development, coordination, and approval processes will adhere to the lead Service procedures.

b. Essential to the T&E WIPT process is the performance of specialized tasks assigned to subordinate working groups (that is, subgroups). The subgroups are necessary to define the details of the T&E program, handle the necessary interfaces with other disciplines not included in the T&E WIPT membership, prepare for testing, and develop supporting T&E documentation. Additionally, the subgroups are required to coordinate and jointly develop T&E needs and identify potential course of action to resolve them. When possible, the T&E WIPT Charter will delineate the planned subgroups. In some cases the subgroups may need to establish their own work groups.

(1) The RAM Working Group, co-chaired by the MATDEV and CBTDEV, will address all RAM T&E issues. The PM, system evaluator, developmental tester, and operational tester, as a minimum, participate on this subgroup. See chapter 5 for more detail.

(2) The Supportability subgroup, chaired by the PM or MATDEV ILS manager, will provide coordination between the T&E WIPT activities and the Supportability IPT. Topics to be coordinated will include all supportability test issues, test requirements, and logistic demonstration requirements contained in the TEMP (AR 700–127). As a minimum, the PM or MATDEV, logistician, and system evaluator participate on this subgroup.

(3) A M&S subgroup, chaired by the PM or MATDEV, will determine those data requirements that can be cost effectively satisfied through validated and accredited M&S rather than by DT or OT testing; use M&S to demonstrate RAM requirements; integrate M&S with the T&E program; obtain empirical data to validate M&S; and determine the appropriate use of accredited M&S to support DT, OT, LFT, and system evaluation. As a minimum, the PM or MATDEV, CBTDEV, TNGDEV, system evaluator, and test representatives participate on this subgroup.

(4) The Threat subgroup, chaired by the TI member of the T&E WIPT, reviews, coordinates, and maintains the threat test support package (TSP). As a minimum, the PM or MATDEV, TI, system evaluator, and test representatives participate on this subgroup.

(5) A live fire test and evaluation (LFT&E) subgroup, when required, chaired by U.S. Army Test and Evaluation Command (ATEC), is formed to prepare the LFT&E strategy and input to the TEMP. Membership typically includes the PM or MATDEV, CBTDEV, TNGDEV, DOT&E, DUSA (OR), system evaluator, vulnerability and lethality analysts, testers, the medical community, the intelligence community, and the system contractor (as required).

c. There are many related disciplines and working groups that have close ties with the T&E WIPT. Their activities occur concurrently and are often combined with the activities of the T&E WIPT. The communication lines between them and the T&E WIPT must be clear and allow for the transfer of information to enhance the progression of work for all disciplines. Some of these closely related disciplines and working groups are listed below.

(1) *Test readiness review.* Testers conduct TRRs at various points leading up to the start of test. MATDEV or PM certifies that the materiel system is ready for test. Threat analyst certifies the threat representation for OT. After coordinating with the doctrine and TNGDEVs, the CBTDEV certifies the readiness of doctrine and organization (D&O) for OT. Trainers certify the readiness of Soldiers and units employing new systems for OT. The test unit certifies its readiness for OT. Testers address the readiness of planning, preparation, and test resources for DT and OT. Essential to the TRR process are entrance criteria established in the TEMP. Specific types of TRRs are—

(a) Operational test readiness review. The operational test readiness review (OTRR) is the forum to assess aspects of a system's readiness to enter OT (such as performance, supportability, training, and doctrine) and the status of planning for and capability to conduct the OT, to include resources and other requirements. Membership includes the PM or MATDEV, operational tester (chair), CBTDEV, TNGDEV or trainer, threat analyst, test unit, logistician, developmental tester, and system evaluator.

(b) Developmental test readiness review. Developmental test readiness review (DTRR) assesses the system's readiness to enter DT and the status of planning for and capability to conduct the DT, to include resources and other requirements. Membership, as a minimum, includes the PM or MATDEV (chair), developmental tester, and system evaluator.

(2) *Data authentication group.* Either the system evaluator or operational tester determines the need for a data authentication group (DAG). By mutual agreement, either the system evaluator or operational tester chairs the DAG

with representatives from required areas of expertise. (See para 6–50.) The DAG meets while operational tests are being conducted to ensure timely exchange of data among all participating organizations/commands and to build a factual database by assisting in data reduction, data analysis, and the investigation of problems surfaced in test data. The group is formed when the evaluation of systems require complex data collection and instrumentation. Its members may also comprise the membership of the RAM Subgroup who participate in the RAM scoring and assessment IPT. Composition of the DAG for an OT is included in the OTP.

(3) *Computer resources working group.* The Computer Resources Working Group is established by the PM or MATDEV after MS B for each materiel system with embedded software to aid in the management of system computer resources. The Computer Resources Working Group assists in ensuring compliance with policy, procedures, plans, and standards established for computer resources. Membership includes the CBTDEV, TNGDEV, MATDEV, developmental and operational testers, system evaluator, and the post deployment software support (PDSS) activities. Members will actively participate in all aspects of the program dealing with computer resources, including software incident reporting and corrective action.

(4) *Supportability Integrated Product Team.* The Supportability IPT is established to coordinate overall ILS planning and execution. Membership includes the PM or MATDEV, developmental tester, operational tester, system evaluator, logistician, and trainer (see AR 700–127).

(5) *Manpower and Personnel Integration Joint Working Group.* The MANPRINT Joint Working Group develops the System MANPRINT Management Plan and coordinates the MANPRINT program. Membership includes the PM or MATDEV, CBTDEV, TNGDEV, system evaluator, logistician, and the personnel community and other organizations as appropriate (see AR 602–2).

(6) *System Safety Working Group.* The System Safety Working Group is chaired by the PM or MATDEV, and provides program management with system safety expertise and ensures enhanced communication between all IPT members. Membership includes the PM or MATDEV, developmental tester, operational tester, system evaluator, and independent Department of the Army (DA)-level oversight (United States Army Safety Center) (see AR 385–10).

**CHARTER OF THE * XYZ_ *
TEST AND EVALUATION WORKING-LEVEL INTEGRATED PRODUCT TEAM
(T&E WIPT)**

1. PURPOSE: Brief statement identifying the system T&E WIPT that is being established.

Example: To formally charter the * XYZ_ * T&E WIPT, comprised of the command representatives for the agencies listed in paragraph 3, below.

2. SCOPE: To develop and maintain T&E strategy. To plan, budget, resource, execute, and conduct a T&E program.

3. MEMBERSHIP: List organizations providing membership, either principal or associate. Include organizational mailing address, office symbol, electronic message address, and DSN and facsimile telephone numbers to facilitate communication between member organizations.

Example:

a. Principal members of the * XYZ_ * T&E WIPT will be composed of one representative (primary) from each of the following:

	NAME	ORG	PHONE	EMAIL
(1) Program/Project/Product Manager (PM)/MATDEV				
(2) CBTDEV/Functional Proponent				
(3) System evaluator				
(4) Developmental Tester				
(5) Operational Tester				
(6) Logistician				
(7) Survivability/Lethality Analysis Directorate				
(8) Trainer				
(9) Threat Integrator				
(10) HQDA Offices				
(a) ASA(ALT)				
(b) CIO/G-6				
(c) DUSA(OR)				
(d) ASA(ALT) ILS (or DCS,G-4)				
(e) DCS,G-1				
(f) DCS,G-2				
(g) DCS,G-3				
(h) DCS,G-8				
(11) For programs on the OSD T&E Oversight List				
(a) DOT&E				
(b) OUSD(AT&L)DS/DT&E				

b. Associate Members: Provide functional or special knowledge, skills, or expert support to the T&E WIPT. Associate members do not have the coordination privilege as the principal members.

4. OBJECTIVE: Specific objective of each T&E WIPT is listed.

Example: The objective of the * XYZ_ * T&E WIPT is to provide a forum for test planning and integration to ensure an adequate and comprehensive test program to fully validate the system.

5. PROCEDURES: The procedures section provides the broad, general guidelines under which the T&E WIPT will operate. The method of calling meetings, representation by members, developing agenda items, and

Figure 2–2. Format of a test and evaluation working-level integrated product team charter

conducting meetings are included. The organization of each T&E WIPT member is shown including the interface with other activities (for example, design engineering, simulation, and targets management). Procedures are also provided for handling open agenda items, resolution of problems and preparation of minutes of each T&E WIPT meeting. Maximum use should be made of correspondence and electronic communication (for example, videoconferences, teleconferences, electronic mail, and facsimile) to resolve issues.

Example:

a. After coordination with principal members, the chairperson will convene a meeting and provide for the recording and distribution of minutes of meetings.

b. Not less than two (2) weeks prior to each meeting, the chairperson will provide each member agency with notification of the time, place, and agenda for the proposed meeting.

c. Member agencies will be responsible for ensuring their own representation and such additional supplementary representation as may be indicated by the agenda.

d. Threat, Supportability, M&S, RAM, LFT&E and training subgroups will be established, as required.

e. Members will be responsible for action items related to their functional areas that are specified on an Action Item List (AIL) that is revised by the organizations' representatives at each meeting. Such additions or deletions as recommended by agency representatives attending will be reviewed by the group and an updated AIL will be provided as part of the minutes.

f. The T&E WIPT members will provide inputs and recommendations with regard to modification and revision of the TEMP.

g. Disagreements that cannot be resolved on matters of substance will be elevated from the T&E WIPT to the IIPT. If the IIPT cannot resolve the disagreement(s), the matter will be brought through the chain of command to the attention of the DUSA(OR) for adjudication.

6. DISTRIBUTION: This section includes distribution to be made of the T&E WIPT Charter, changes thereto, minutes of meetings, plans, and reports.

Example:

a. This charter, minutes of all meetings, and all issues of the * **XYZ** _* T&E WIPT AIL will be distributed to each * **XYZ** _* T&E WIPT principal member within ten (10) working days after the meeting.

b. If the minutes do not adequately reflect a member's understanding of what was accomplished at a T&E WIPT meeting, or if a member organization's position changes, this should be brought to the attention of the chairperson for correction or added as an action item to the next T&E WIPT Agenda within two (2) weeks after receipt of the minutes.

c. Additional supplemental distribution of meeting minutes and AIL will be as recommended by the group.

d. Copies of T&E documentation, both government and contractor, will be provided to all T&E WIPT members.

e. Specific points of contact and their addresses are provided as an appendix.

7. Based on concurrence by the principal T&E WIPT members, this charter is approved.

Signature Block/Date	Signature Block/Date
T&E WIPT Chair	PM * **XYZ** _*

Figure 2–2. Format of a test and evaluation working-level integrated product team charter—Continued

Chapter 3
Test and Evaluation Master Plan

3–1. Test and evaluation master plan procedures

a. This chapter provides procedural guidance for preparing, staffing, and gaining approval of the TEMP. Detailed guidance on format, content, review, and approval procedures to be followed by all Army programs in preparation of the TEMP is also included in this chapter.

b. All acquisition programs are supported by an acquisition strategy that reflects a comprehensive and efficient T&E program. To accomplish this task, each acquisition program/system will have a single TEMP, except those involving the use of investigational drugs, biologicals, and devices in humans that fall under Parts 50, 56, and 312, Title 21, Code of Federal Regulations. (See AR 73–1.)

c. TEMP requirements are summarized below:

(1) The TEMP is the basic planning document for all life cycle T&E related to a particular system acquisition and is used by decision making bodies in planning, reviewing, and approving T&E activities. The TEMP documents T&E planning and requires executive level approval before proceeding to program initiation and subsequent MS and the FRP DR. The approved TEMP is the overarching T&E document used by the T&E community to generate detailed T&E plans and to ascertain schedule and resource requirements associated with the T&E program. Since the TEMP charts the T&E course of action during the system acquisition process, all testing, data generation/gathering, and other evaluation events/activities planned that impact on program decisions are outlined.

(2) The TEMP is a living document that summarizes program schedule, test management strategy and structure, and required resources to address and assess the adequacy to achieve the requirements stated in the—

(a) COIC, to include KPPs and other operational requirements (that is, threshold and objective levels from the ORD).

(b) CTPs.

(c) Evaluation requirements (for example, MOE, MOS, MOP, and criteria, when applicable).

(d) Major decision points.

(3) An approved Army TEMP is required before an OTP for a test supporting system acquisition can be included in the Five-Year Test Program (FYTP).

(4) The TEMP addresses the T&E to be accomplished in each planned program phase. The TEMP can jointly address DT & OT in a consolidated Part III–Integrated Test and Evaluation.

(5) The body of a TEMP should be reflective of the amount of testing required and complexity of the program. Being a management plan, the target size of a TEMP should be approximately 30 pages, including pages for figures, tables, matrices, and so forth. Although annexes and attachments are excluded from the 30-page limit, their size should be kept to a minimum. The TEMP must provide a clear and adequate definition of the system's T&E strategy and requirements being addressed to constitute agreement on key elements for resourcing and execution.

(6) Classified TEMPs must be clearly marked as to the classification level and those submitted for HQDA and/or OSD approval must contain all classified data and attachments. A draft TEMP forwarded electronically for review must be done with any classified information omitted, with the classified information sent via secure means (see AR 380–5).

(7) A capstone TEMP is required when a program consists of a collection of individual systems, either as a family-of-systems or as a system-of-systems with requirements stated in a capstone requirements document (CRD). A capstone TEMP integrates the T&E program planned for the entire family or system-of-systems. When appropriate, an annex to the basic capstone TEMP will address individual system-unique content requirements. The need for a capstone TEMP depends upon the degree of integration and interoperability required to satisfy the total system's interoperability KPP, associated information exchange requirements (IERs), and other appropriate operational performance parameters (for example, Joint Technical Architecture (JTA) compliance). The body of a capstone TEMP should be approximately 30 pages, including pages for figures, tables, matrices, and so forth. Each individual system TEMP will be a complete stand-alone document that is annexed to the capstone TEMP.

d. The TEMP is prepared by the MATDEV with support of and in coordination with the other core and principal T&E WIPT members and submitted to the appropriate TEMP approval authority. The initial TEMP is required for program initiation, normally MS B, and is updated, as a minimum, at MS C and the FRP DR for the initial acquisition or increment. TEMP updates reflect planning for each increment under evolutionary acquisition and require approval prior to DRs authorizing execution of each increment as well as updates at MS and FRP DRs for each increment upgrade. The TEMP focuses on the overall structure, major elements, and objectives of the T&E program and is consistent with the acquisition strategy, approved ORD, and other program documentation (for example, C4ISP). An Army TEMP 101 Brief, developed in coordination with the Test and Evaluation Managers Committee (TEMAC), is

maintained by TEMA and is located at www.hqda.army.mil/tema. The TEMP Checklist, appendix B to this pamphlet, may be used as a guide for TEMP development, review, and staffing.

3–2. Test and evaluation master plan considerations

a. The TEMP must include at least one CTP and one operational effectiveness issue for the evaluation of interoperability, to include both intra-Army interoperability certification by the Central Technical Support Facility (CTSF) and joint interoperability certification by the Joint Interoperability Test Command (JITC). The TEMP should reference and extract requirements from the appropriate MNS, CRD, ORD, C4ISP, and integrated architectures. The Joint Staff, or DCS, G–8 in the case of Army-only materiel and tactical C4I/IT programs, will ensure that all MNS, CRD, and ORD contain specific, testable, and measurable interoperability requirements by coordination with and involvement of appropriate T&E organizations in the requirement generation and approval process. The Joint Staff, USD (AT&L), and Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD (C3I))/DoD CIO, or the CIO/G–6 in the case of Army-only non-tactical C4/IT programs, will ensure that the C4ISP and integrated architectures reflect the appropriate family-of-systems context to support the system's interoperability requirements. The system evaluator and testers, in coordination with the MATDEV and CBTDEV or FP for non-tactical C4/IT programs, TNGDEV, and CIO/G–6, should develop the test procedures and effectiveness measures based on the requirements and expected concepts of operations for the systems. Both developmental and operational test plans should specify interoperability test concepts. If not a part of the COIC, the system evaluator for Army programs may include the effectiveness measures in its AIs for evaluation through the SEP and test/EDPs.

b. Early T&E activities will associate MOEs, MOSs, MOPs, risks with the needs depicted in the MNS, and with the objectives and thresholds addressed in the AoA. Thresholds are defined in the ORD and acquisition program baseline (APB) as these documents become available. Criteria, quantitative when possible, will determine hardware, software, life cycle test facility base infrastructure (to include hardware-in-the-loop (HWIL) and training system requirements), and system maturity and readiness to proceed through the acquisition process. The various approved KPPs and the MOE/MOS used in the AoA and during T&E will remain linked. This linkage is depicted in the TEMP, Attachment 1—Requirements/Test Crosswalk Matrix. Operational scenarios and conditions must also remain linked in order to compare results. AoA and T&E operations must remain linked to provide data for the VV&A of models and simulations, provide for model-test-model applications, and otherwise foster exchange of system data between analyst, tester, and evaluator to promote understanding of a system's effectiveness, suitability, and survivability.

3–3. Test and evaluation master plan requirements

a. TEMP format considerations include—

(1) Army TEMP policy requires that the Defense Acquisition Guidebook format be followed. Within this format, the level of detail is unique for each program. Tailoring of TEMP contents within this format is encouraged. The level of TEMP detail is directly related to the proposed T&E strategy; complexity of the T&E effort needed to verify attainment of technical performance; technical specifications, objectives, safety, and supportability; and to support the evaluation/assessment of the operational effectiveness, suitability, and survivability of the system. The content guidance contained in the following sections is intended to assist the T&E WIPT and the TEMP approval authority in developing a TEMP that reflects an adequate and efficient T&E program.

(2) Appendix C provides various TEMP approval page formats to be used.

(3) For TEMPs not requiring HQDA or OSD approval (generally ACAT III programs), additional tailoring is authorized. Although the general format in the Defense Acquisition Guidebook is to be followed, tailoring is allowed to reduce development effort and minimize the size of the TEMP. For example, the following tailoring is permitted—

(a) Part I, System Introduction, paragraph d, Measures of Effectiveness and Suitability. It is sufficient to reference the ORD.

(b) Part II, Integrated Test Program Summary. See appendix D, figure D–1 (this summary does not have to be rigidly followed). A program schedule can be used as long as test, data collection/gathering, and other evaluation activities/events are identified. Funding information should be as complete as possible. T&E WIPT member responsibilities do not have to be described in detail. Referencing the charter is sufficient.

(c) Parts III and IV may be consolidated into a single section titled "Integrated Test and Evaluation." This does not just apply to ACAT III programs when DT and OT are combined.

(d) Part IV, Operational Test and Evaluation Outline and Live Fire Test and Evaluation Paragraphs. Most ACAT III programs are not required to execute a formal LFT&E program unless they meet the definition of a covered system or major munitions program as defined in 10 USC 4172. Live fire tests are those tests conducted to gain insight into warhead/target terminal effects (for example, lethality/vulnerability given a hit) and should not be confused with live munitions or missile firings conducted during other DT and OT events (for example, hit probability, or reliability).

b. TEMP development input is appropriate T&E information necessary to ensure the COIC, ORD, CTP, and previous identified deficiencies and requirements are being addressed or have been satisfied. Input is generally provided by the T&E WIPT. See chapter 2, above, for T&E WIPT composition, roles, and functions. Other Government and contractor activities may also provide input to the TEMP, when appropriate. Comments are integrated in the TEMP by the PM, who has primary responsibility for TEMP preparation, staffing, and update in coordination with other core T&E WIPT members. The MATDEV develops a TEMP Coordination Sheet, with the signature blocks of all principal T&E WIPT members. The Coordination Sheet accompanies the TEMP when forwarded for TEMP approval.

c. A strawman TEMP can be prepared by the PM supported by the core T&E WIPT members for review, discussion, and consideration at the initial T&E WIPT meeting to facilitate T&E strategy discussions and the development of the initial TEMP. The strawman TEMP should be provided to the T&E WIPT members not later than 15 days prior to the initial T&E WIPT meeting. A strawman TEMP will not be cause to limit consideration of principal member proposed alternatives.

d. An initial TEMP is submitted and approved to support program initiation. Since not all information may be available, the initial TEMP should so note the missing information and identify the date when the information will become available.

e. TEMPs requiring HQDA approval include—

(1) Programs on the OSD T&E Oversight List, which is jointly published annually, by the DOT&E and the Director, Defense Systems, Office of the Under Secretary of Defense (Acquisition, Technology and Logistics) OUSD (AT&L) in consultation with the T&E executives of the cognizant DoD components. These programs require OSD TEMP approval and forwarding of other T&E documentation to OSD. For programs initially designated on the OSD T&E Oversight List, an Army approved TEMP is due to OSD within 90 days of the initial designation.

(2) A TEMP submitted for HQDA or OSD will comply with the milestone documentation submission schedule. The Defense Acquisition Guidebook encourages programs subject to Defense Acquisition Board (DAB) review to submit the TEMP to OSD 30 days prior to the DAB committee review. Programs on the OSD T&E Oversight List that are subject only to internal Army Systems Acquisition Review Council, that is, ACAT IC and II must submit the TEMP to OSD 30 days prior to the MS review. If the various HQDA offices have not been included in the initial T&E WIPT and TEMP staffing processes, an additional 20 days are needed for HQDA review and DUSA (OR) approval prior to gaining HQDA TEMP approval. Programs subject to Missile Defense Agency coordination and approval require an additional 14 days for Missile Defense Agency staffing after DUSA (OR) concurrence and prior to submission to OSD.

f. A TEMP is updated prior to Milestone C and the FRP DR (as required in DoDI 5000.02), when the APB has been breached, when the associated ORD or C4ISP has been significantly modified, or on other occasions when the program has changed significantly. Evolutionary acquisition programs may require additional updates to ensure that the TEMP reflects the currently defined program. When a baseline breach occurs, the TEMP will be updated within 120 days of the date of the PM's Program Deviation Report. When a program changes significantly, the TEMP due date will be negotiated between the PM, TEMA, and the DUSA (OR). In the case of programs on the OSD T&E Oversight List, the negotiations will take place between the PM, DUSA (OR), TEMA, DOT&E, and Deputy Director, Development Test and Evaluation/Defense Systems (DD, DT&E/DS) OUSD (AT&L).

(1) There are three forms a TEMP update can take—

(a) Page changes. Page changes are the preferred approach, when appropriate, because they reduce the effort to review the TEMP, resulting in a speedier review and approval process. Page changes will be submitted as either hardcopy remove and replace changed pages to a standing version of a TEMP or as a file that uses word processing change markings so as not to affect the integrity of the basic document. When page changes are used, each changed page will footnote the current date and change. A signed coordination sheet and approval page must accompany page changes more detailed than an editorial correction to sentences, and other similarly minor instances.

(b) Revisions (rewrites). A TEMP revision is required to address comments received during the review and approval process subsequent to T&E WIPT coordination. TEMPs for ACAT III programs are not subject to the procedures for revision unless they are on the OSD T&E Oversight List and/or when senior management's objections reverse the T&E WIPT coordination. Changes to a TEMP are annotated by change bars in the outside margin. A brief synopsis of how issues and comments were addressed and/or why specific changes were made will accompany the revision. Each changed page will footnote the revision number and current date. For all revisions, T&E WIPT members will be provided a copy of the changes for comment or concurrence to ensure changes are acceptable.

(c) "No change" memorandum. The no change memorandum, when used for ACAT I, II, and other programs on the OSD T&E Oversight List as well as Army and OSD major automated information system (MAIS) programs, is prepared by the PM, fully coordinated, and forwarded to TEMA for DUSA (OR) approval and subsequent forwarding to OSD, as appropriate.

(2) Coordination and Approval of TEMP Updates. Regardless of the TEMP update form, it requires a completed coordination and approval process. Coordination with the T&E WIPT members is recorded by executing a T&E WIPT Coordination Sheet. T&E WIPT coordination signatures assist in expediting the TEMP approval process as well as to recognize the key participants in the TEMP development process. If not obtainable at the T&E WIPT "signing party," signatures can be obtained via facsimile or through a scanned PDF file on separate pages for retention by the T&E WIPT chair.

(a) A new TEMP approval page will be executed by the PM, PEO (or developing agency), U.S. Army Training and Doctrine Command (TRADOC) (or FP for non-tactical C4/IT systems) and ATEC for all revisions resulting for HQDA and OSD approval.

(b) The update will be forwarded by memorandum to TEMA for HQDA review and DUSA (OR) approval and forwarding by TEMA to OSD, as necessary. The memorandum will record that T&E WIPT member coordination was obtained and will enclose the properly executed TEMP approval page.

g. Documents that should accompany a TEMP when submitted for HQDA approval include—

(1) A copy of the approved MNS or ORD and validated STAR should be forwarded electronically with the TEMP, unless previously distributed. Classified documents will be sent via the Secret Internet Protocol Router Network (SIPRNET) system or by classified regular mail, not electronically on unclassified machines.

(2) In case of a TEMP update, if support documentation is final and has not changed since the last TEMP approval, a statement will accompany the TEMP attesting to that fact; copies of the documents need not be forwarded. The statement should cite the date, version and/or change number for the most current documents.

h. All documents referenced in the TEMP must be available for submission to HQDA or OSD on request.

i. The request for delay in submitting a TEMP is prepared by the PM. The request for delay will be forwarded to TEMA for forwarding to OSD and DUSA (OR) approval, as necessary. For programs requiring the Missile Defense Agency approval, TEMA will submit a request for delay to the Missile Defense Agency for approval or to OSD if OSD approval is required. In all cases, the reason for the delay must be clearly explained. Delays for administrative reasons are generally not accepted.

j. At the PM's discretion, copies of the approved TEMP can be distributed. If bound, a TEMP must allow for easy insertion of page changes; spiral binding, square, or glue bindings are discouraged. TEMPs submitted for HQDA and OSD approval must contain all classified data and annexes/attachments.

k. When system development is complete and COIC are satisfactorily met or resolved, including the verification of deficiency corrections, a TEMP update is no longer required. Specifically, for programs—

(1) OSD T&E Oversight. A request to delete the program from the OSD T&E Oversight List should be prepared by the PM or MATDEV and forwarded through the PEO (or developing agency if not a PEO managed program) to TEMA for forwarding to the DD, DT&E/DS for OSD review and approval. For Missile Defense Agency programs, the request will be sent to the Missile Defense Agency Acquisition Executive by TEMA for forwarding to OSD for approval. The request must be coordinated with TRADOC and ATEC or U.S. Army Space and Missile Defense Command (SMDC) before forwarding to TEMA.

(2) Non-OSD T&E Oversight. A request to defer further updates should be prepared by the MATDEV, coordinated with the T&E WIPT and approved by the TEMP approval authority. Approval should be made a matter of record.

l. Programs possessing the following attributes may no longer require a TEMP update—

(1) A fully deployed system with no operationally significant product improvements or increments remaining.

(2) FRP ongoing, fielding initiated with no significant deficiencies observed in production qualification/verification test results.

(3) A partially fielded system in early production phase having successfully accomplished all DT and OT objectives.

(4) Programs for which planned T&E is only a part of routine aging and surveillance testing, service life monitoring, or tactics development.

(5) Programs for which no further OT or LFT is required by the Army, Joint Chiefs of Staff, or OSD.

(6) Programs for which future testing (for example, product improvements or increments) has been incorporated in a separate TEMP.

m. Development of the TEMP begins with the establishment and chartering of the T&E WIPT by the PM. The T&E WIPT Charter will identify the role and responsibilities of all agencies participating in T&E. See AR 73–1 and figure 2–2 for a sample format T&E WIPT Charter.

3–4. Principal test and evaluation master plan responsibilities

The PM, or in some cases the MATDEV, has the overall responsibility to produce the TEMP. The ideal method to develop a TEMP is for concurrent TEMP development by the PM, and core T&E WIPT members (that is, PM T&E

lead, CBTDEV or FP, and system evaluator). Input from the other T&E WIPT members comes during the review cycle when the TEMP is staffed for coordination. The responsibilities to maintain TEMP interface between principal T&E WIPT members by TEMP paragraph are shown in table 3–1.

a. Program, project, and product manager. Primary TEMP author: Part I, System Introduction, Part II, Integrated Test Program Summary, Part III, Developmental Test and Evaluation Outline (documenting tests that provide information directly to the PM, for example, contractor tests) and Part V, T&E Resource Summary.

b. Combat developer, training developer, and functional proponent. Provide Part I, System Introduction—Mission Description and Measures of Effectiveness and Suitability; Part IV, Operational Test and Evaluation Outline—Critical Operational Issues and Criteria; and input to Part V, T&E Resource Summary and Manpower/Personnel Training. Provide inputs on force development test or experimentation (FDT/E), concept experimentation program (CEP), and Battle Lab experimentation for inclusion in Parts II and IV as necessary.

c. Evaluator and testers. Provide input to Part II, Integrated Test Program Summary and Part III, Developmental Test and Evaluation Outline. Provide Part IV, Operational Test and Evaluation Outline and primary input to Part V, T&E Resource Summary.

d. Threat integrator. Provide input to Part I, System Introduction, System Threat Assessment.

Table 3–1
Test and evaluation master plan preparation responsibility matrix

TEMP part and section	PM	CD/FP	TI	T&E Activity	Logistics
Part I. System Introduction					
a. Mission Description	S	P			
b. System Description	P	S			
c. System Threat Assessment	S		P	S	
d. Measures of Effectiveness and Suitability	S	P		S	S
e. Critical Technical Parameters	P	S		S	S
Part II. Integrated Test Program Summary					
a. Integrated Test Program Schedule	P	S		S	S
b. Management	P	S		S	S
Part III. Developmental Test and Evaluation Outline					
a. Developmental Test and Evaluation Overview	P			S	S
b. Future Developmental Test and Evaluation	P			S	S
Part IV. Operational Test and Evaluation Outline					
a. Operational Test and Evaluation Overview	S			P	S
b. Critical Operational Issues and Criteria	S	P		S	
c. Future Operational Test and Evaluation	S	S		P	S
d. Live Fire Test and Evaluation	S			P	
Part V. Test and Evaluation Resource Summary					
a. Test Articles	S			P	S
b. Test Sites and Instrumentation	P	S		P	S
c. Test Support Equipment	S		S	P	S
d. Threat Representation	S		S	P	
e. Test Targets and Expendables	P		S	P	
f. Operational Force Test Support			S	P	
g. Simulations, Models and Testbeds	P	S		P	
h. Special Requirements	S			P	

Table 3–1
Test and evaluation master plan preparation responsibility matrix—Continued

i. T&E Funding Requirements	P			P	
j. Manpower/Personnel Training		P		P	S
Annex A Bibliography	P	S	S	S	S
Annex B Acronyms	P	S	S	S	S
Annex C Points of Contact	P	S	S	S	S
Attachment 1: Requirements/Test Crosswalk Matrix	P	S		S	
Other Annexes/Attachments	P				

P: Principal responsibility; PM: Program manager; LOG: Logistician; TI: Threat integrator; S: Support responsibility; CD/FP: Combat developer/functional proponent

3–5. Test and evaluation master plan review and approval process

a. General review and approval procedures involve—

(1) *Review and concurrence.* Upon development and coordination with the T&E WIPT members (see fig 3–1), the TEMP is submitted for principal signatory review and concurrence. This review and approval process varies depending on TEMP approval authority. Changes required to the TEMP as a result of review must be restaffed with the T&E WIPT and other principal signatories. Re-staffing time is to be held to a minimum, that is, no more than 15 calendar days. The TEMP checklist provided as appendix B may be used as a guide during the TEMP review and approval process.

(2) *Empowerment for approval page.* T&E WIPT members representing organizations included on the approval page are encouraged to attend the final T&E WIPT empowered to sign the approval page for their organization. This requires the representative to have staffed the document throughout their organization and received authorization from the signature authority to sign the TEMP. Doing so dramatically decreases the TEMP staffing time and negates potential submission delays to HQDA and/or OSD.

b. TEMP staffing for OSD T&E oversight materiel and tactical C4I/IT programs (ACAT I–III). (See fig 3–2.)

(1) The PM signs in the "submitted by" signature block on the approval page and forwards the TEMP concurrently to the PEO (developing agency, if not under PEO structure), TRADOC, and ATEC (or their designees) for concurrence. The PM then forwards the fully signed TEMP to TEMA for HQDA staffing (if not incorporated in the T&E WIPT process as described in chapter 2, above) and approval by the DUSA (OR). This concurrence and approval process should take no more than 30 calendar days.

(2) Upon Army approval, TEMA forwards the TEMP by transmittal memorandum to the DD, DT&E/DS for OSD review and approval.

(3) A TEMP is approved when signed by the DOT&E and D, DS. The OSD goal is to provide formal approval or comments for TEMP modifications within 30 calendar days after receipt.

(4) The OSD approval memorandum and signed TEMP approval page (see fig C–1) are forwarded by TEMA to the PM for inclusion in the TEMP and is attached to the front cover.

c. TEMP staffing for Missile Defense Agency programs (see fig 3–3).

(1) After the T&E WIPT chair provides a fully coordinated TEMP to the PM, the PM signs in the "submitted by" signature block of the approval page and forwards the TEMP concurrently to the PEO Air and Missile Defense (AMD), TRADOC, and ATEC for concurrence. The PM forwards the fully coordinated and signed TEMP to TEMA for HQDA staffing (if necessary) and concurrence by the DUSA (OR). Upon Army concurrence, TEMA forwards the TEMP to the Missile Defense Agency program integrator. This concurrence process should be accomplished within 30 calendar days.

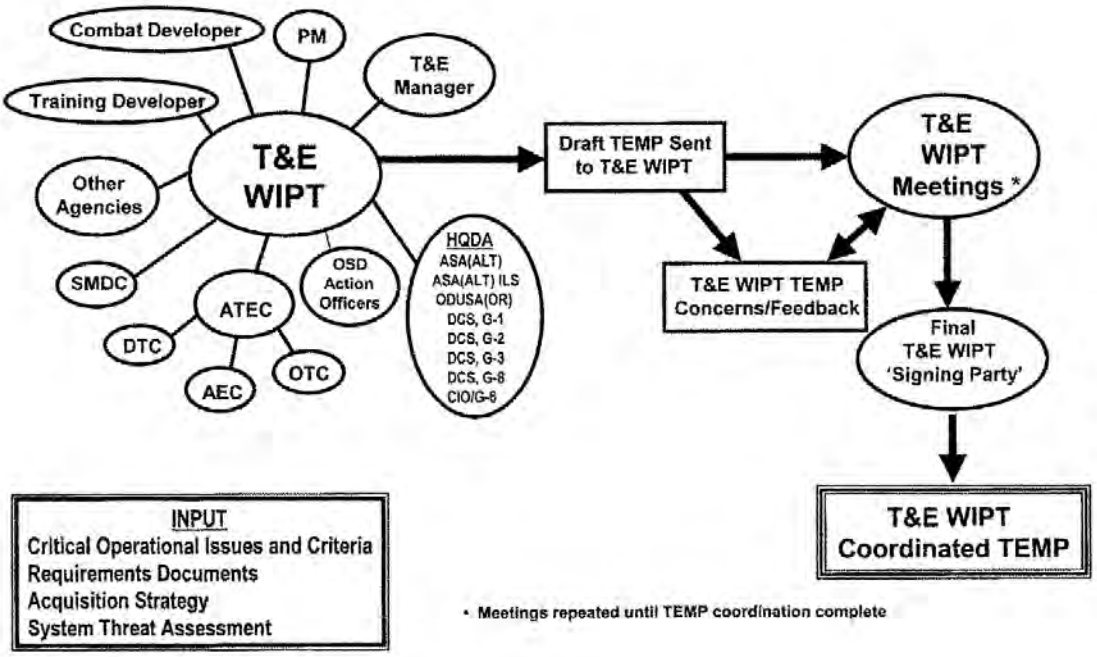


Figure 3–1. Test and evaluation master plan development and test and evaluation working-level integrated product team coordination process

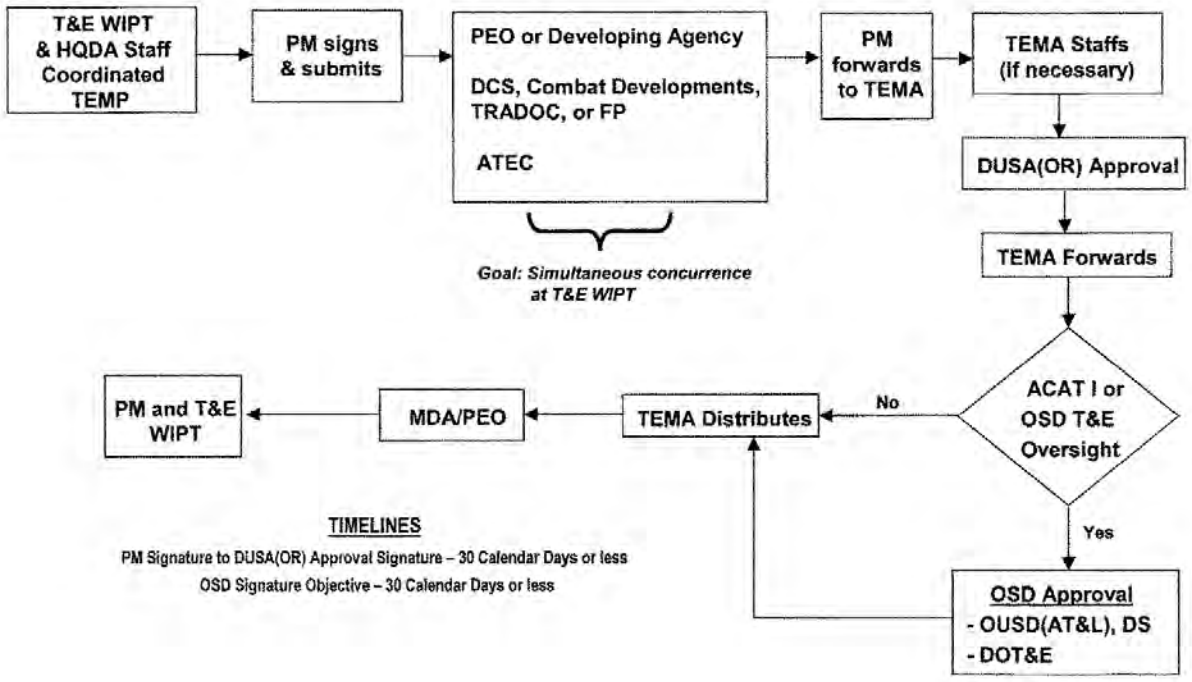


Figure 3–2. Test and evaluation master plan staffing for Office of the Secretary of Defense test and evaluation oversight programs

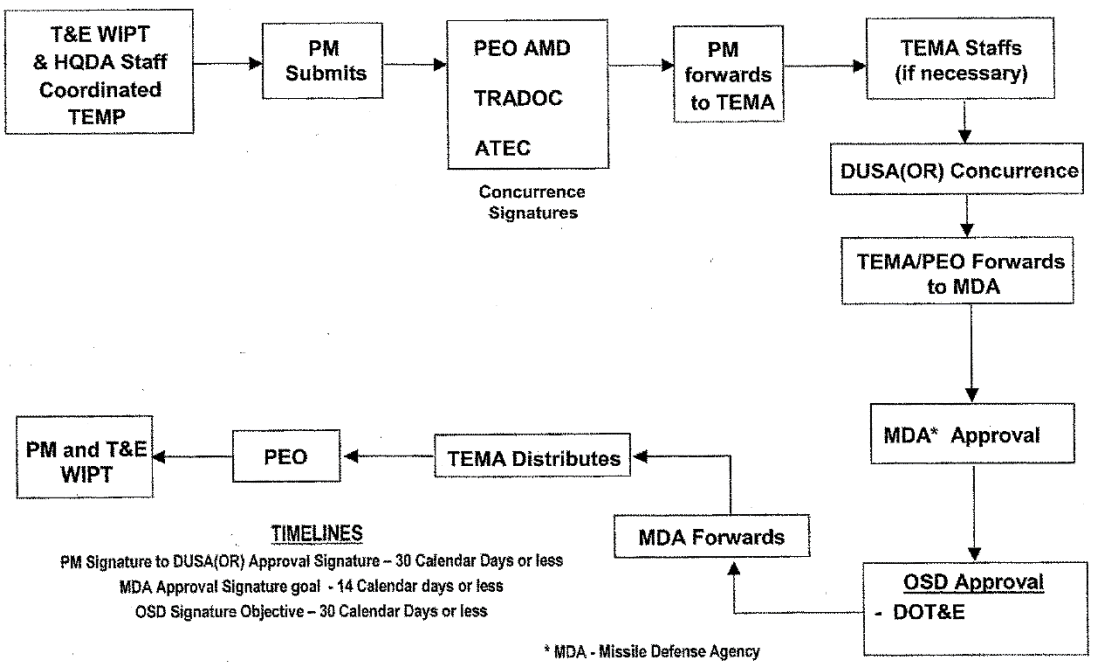


Figure 3–3. Test and evaluation master plan staffing for Missile Defense Agency programs

(2) The program integrator, through the Missile Defense Agency T&E Directorate, obtains Missile Defense Agency review and approval. This coordination process should take no more than 14 calendar days.

(3) Upon Missile Defense Agency approval, the Missile Defense Agency program integrator forwards the TEMP to the DOT&E for OSD review and approval.

(4) The TEMP is approved when signed by the DOT&E. The OSD goal is to provide formal approval or comments for TEMP modifications within 30 calendar days from receipt. (See app C, fig C–2.)

(5) The OSD approval memorandum and signed TEMP approval page are forwarded to the Missile Defense Agency program integrator for inclusion in the TEMP for final distribution. The total staffing process, from PM submission until OSD approval, should not exceed 74 calendar days.

d. TEMP staffing for multi-Service OSD T&E oversight materiel and tactical C4I/IT programs—Army lead (ACAT I–III) (see fig 3–4). Same as detailed in paragraph 3–5*b*, above, except—

(1) After the T&E WIPT chair provides a fully coordinated TEMP to the PM, the PM or developing agency forwards the TEMP concurrently to the PEO, TRADOC, ATEC and the participating Service operational test agencies (OTAs) and participating Service PEO or developing agency and user's representative for concurrence. This concurrence process should take no more than 20 calendar days and supplements the coordination accomplished at the T&E WIPT level.

(2) The PM provides a copy of the fully coordinated and concurred TEMP to TEMA for forwarding to the other Services' TEMP approval authorities for their component approval. A copy of the MNS, STAR, and ORD, or a statement of currency if documents were previously submitted and are still current should be sent as needed. Upon other Services' component approvals, the TEMP is delivered to TEMA for approval by the DUSA (OR). This process should not exceed 10 calendar days. TEMA forwards the Army approved TEMP to the DD, DT&E/DS for OSD review and approval.

(3) If the multi-Service program is not on the OSD T&E Oversight List, the PM forwards the TEMP to the Army MDA for approval. Upon MDA approval, the PM distributes the TEMP. The total process should not exceed 60 calendar days.

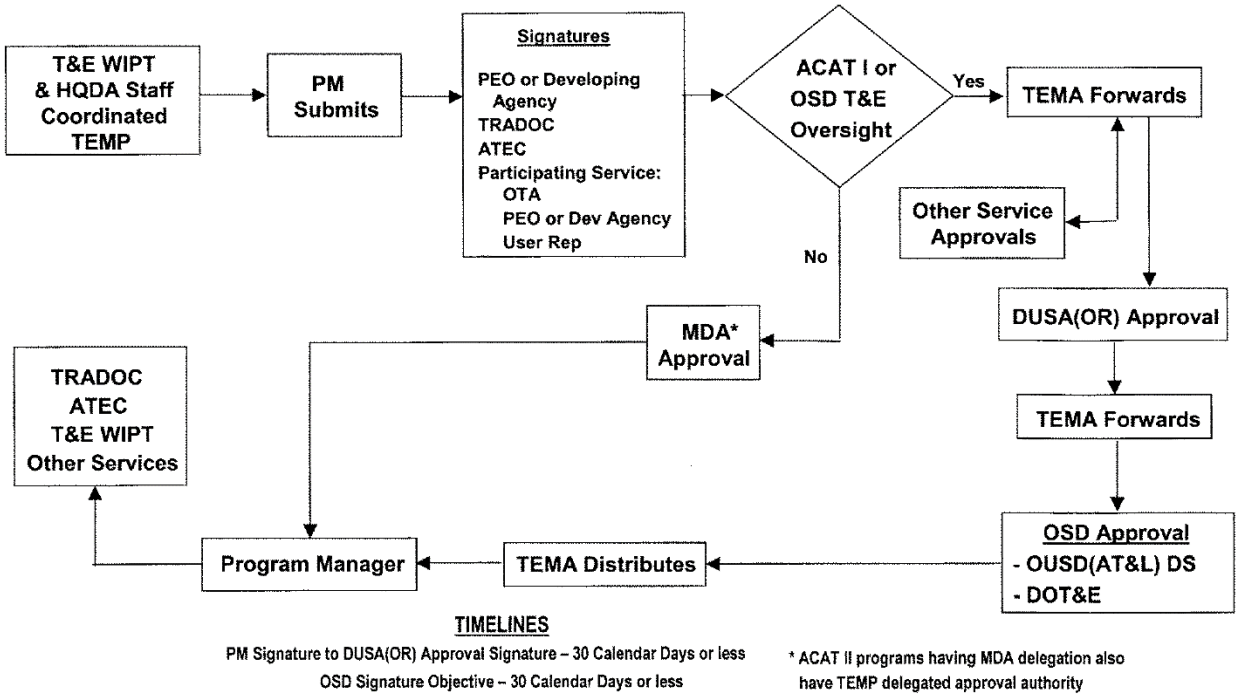


Figure 3–4. Test and evaluation master plan staffing for multi-Service Office of the Secretary of Defense test and evaluation oversight programs—Army lead

(4) The approval page format is shown at figure C–3. If there is more than one participating Service or agency, a separate approval page for each Service or agency should be prepared. The approval page should include the concurrence signature block for each Service or agency PEO, user representative, the OTA, and the Service or agency TEMP approval authority. Both the U.S. Air Force and the U.S. Navy have two TEMP approval authorities. For the Air Force, the Assistant Secretary of the Air Force (Acquisition) and the Director, Air Force Test and Evaluation, U.S. Air Force approve the TEMP. For the Navy, the Assistant Secretary of the Navy (Research, Development, and Acquisition) and the Director, Test and Evaluation and Technology Requirements, Office of the Chief of Naval Operations, approve the TEMP.

(5) As necessary, TEMP information to support Joint Requirements Oversight Council (JROC) will be made available.

e. TEMP staffing for multi-Service OSD T&E oversight materiel and tactical C4I/IT programs—Army Participant. (See fig 3–5.)

(1) The TEMP is prepared according to lead Service or agency procedures. Army unique COIC are to be provided for inclusion as an annex to the TEMP.

(2) The lead Service PM forwards the T&E WIPT (or equivalent) coordinated TEMP to the lead Service PEO for concurrence. The lead Service PEO sends the TEMP to the Army PEO or developing agency for signature and to secure ATEC and TRADOC concurrence on the approval page. For those multi-Service programs where a separate Army T&E WIPT is convened and TEMP coordination is documented on a T&E WIPT Coordination Sheet, the responsible Army PEO or PM should forward the T&E WIPT concurrence to TEMA to support HQDA review (if necessary) and approval by the DUSA (OR).

(3) The lead Service provides the TEMP to TEMA for HQDA staffing and approval by the DUSA (OR). This coordination process is to be accomplished within 20 calendar days.

(4) The Army approved TEMP is returned by TEMA to the lead Service (see fig C–3).

(5) The lead Service acquisition executive forwards the TEMP to the DD, DT&E/DS for OSD review and approval.

(6) The OSD approved TEMP is distributed by the lead Service PEO. Each participating Service receives a copy of the OSD TEMP approval memorandum. The total process time should not exceed 50 calendar days.

(7) As necessary, TEMP information to support JROC will be made available.

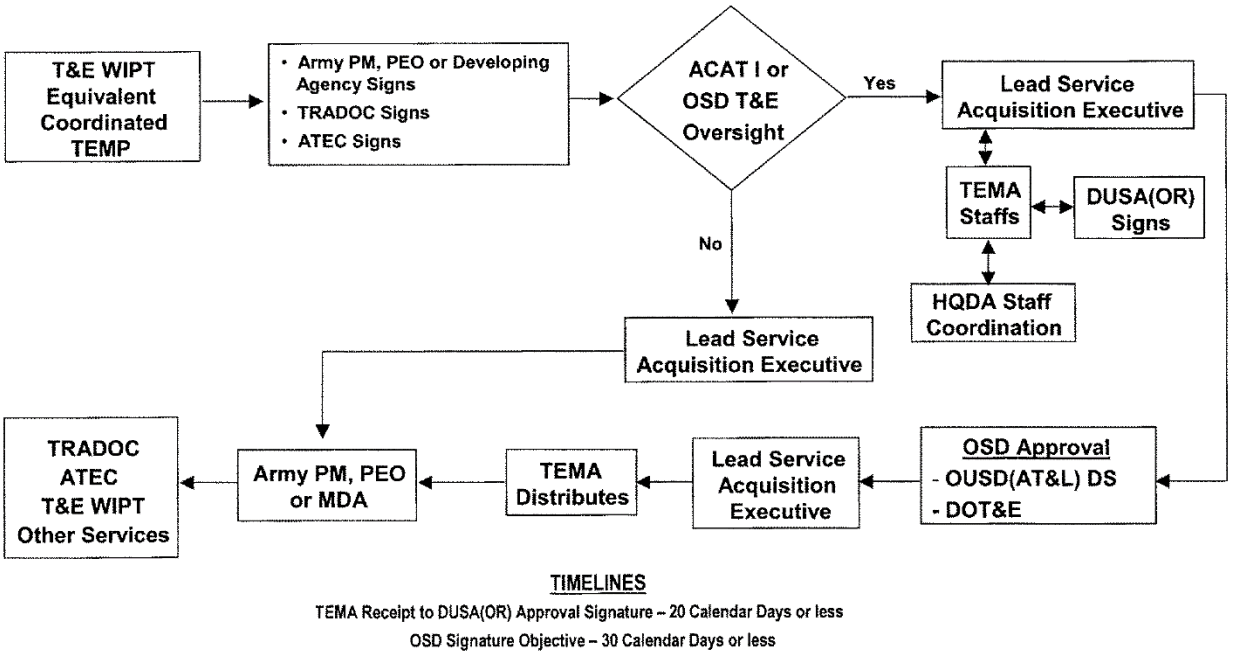


Figure 3–5. Test and evaluation master plan staffing for multi-Service Office of the Secretary of Defense test and evaluation oversight programs—Army Participant

f. TEMP staffing for ACAT II and Army special interest programs, non-OSD T&E oversight.

(1) After the T&E WIPT chair provides a fully coordinated TEMP to the PM, the PM signs in the "submitted by" signature block on the approval page and forwards the TEMP concurrently to the PEO (developing agency, if not under PEO structure), TRADOC, and ATEC for concurrence. If the Army Acquisition Executive (AAE) delegates the MDA to a PEO, then the PM forwards the TEMP to the delegated MDA for approval. If the AAE retains authority over the program, then the PM forwards the signed TEMP to TEMA for HQDA staffing and approval by the DUSA (OR). This process should take no more than 30 calendar days.

(2) The Army approved TEMP is returned to the PM for distribution.

(3) This process is reflected at figure 3–2, when AAE is MDA, and figure 3–6, when MDA is delegated to a PEO.

(4) The approval page format is shown in appendix C, figures C–1 or C–4.

g. TEMP staffing for multi-Service non-OSD T&E oversight ACAT II programs for Army-lead and MDA is the AAE.

(1) After the T&E WIPT chair provides a fully coordinated TEMP to the PM, the PM signs in the "submitted by" signature block on the approval page and forwards the TEMP concurrently to the PEO (developing agency, if not under PEO structure), TRADOC, ATEC, and the participating Service OTAs, participating Service PEOs, or developing agencies and user's representatives for concurrence. This coordination process should take no more than 20 calendar days and supplements the coordination accomplished at the T&E WIPT level.

(2) The PM provides a copy, to include one for each participating Service, of the signed TEMP to TEMA for HQDA staffing and other Service approval. The TEMP is then submitted for approval by the DUSA (OR).

(3) The DUSA (OR) approved TEMP is returned by TEMA to the PM for distribution.

(4) This process is reflected at figure 3–6 when the MDA is retained by the AAE.

(5) The approval page format is shown in appendix C, figure C–5.

h. TEMP staffing for non-OSD T&E oversight ACAT III (to include multi-Service) and Army special interest programs. (See fig 3–6.)

(1) T&E WIPT members should staff the TEMP within their organization to ensure complete review and concurrence during the initial 30 calendar day TEMP review period. Substantive issues should be surfaced and resolved at the T&E WIPT. T&E WIPT member coordination constitutes organization concurrence.

(2) Approval is held in abeyance pending T&E WIPT member senior management review. The review period for ACAT III programs is 20 working days after concurrence by an organization's T&E WIPT member. On expiration of

the review period, the TEMP approval authority signs the TEMP as approved and executable, provided no objections are received from T&E WIPT organizations. The TEMP approval authority is the MDA.

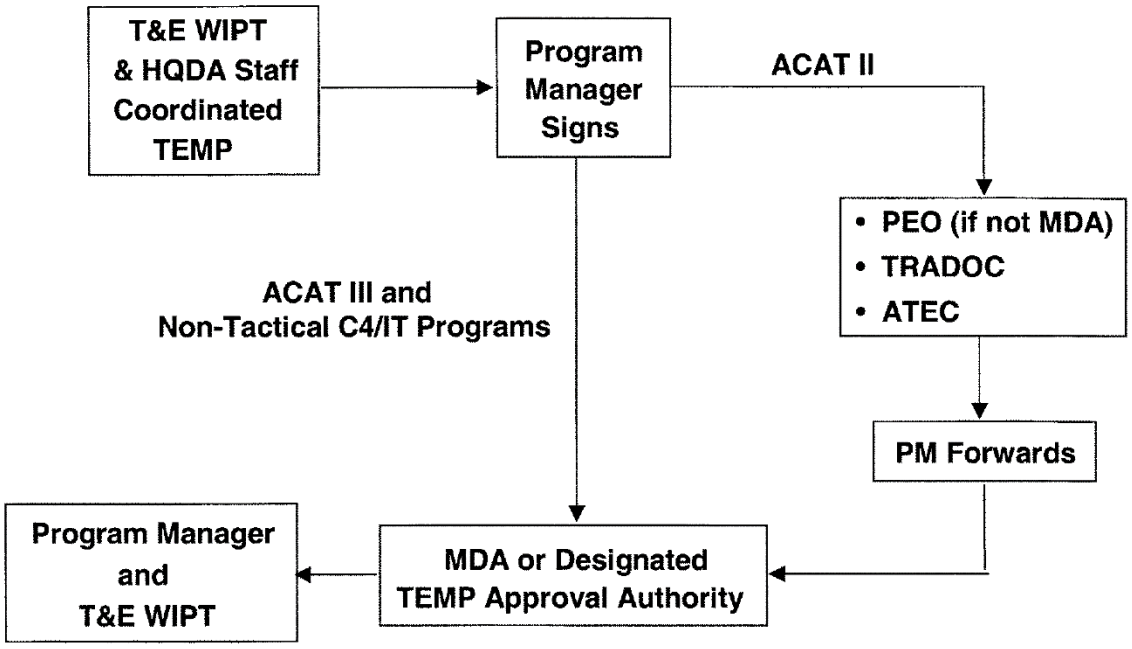


Figure 3–6. Test and evaluation master plan staffing for non-Office of the Secretary of Defense test and evaluation oversight Acquisition Category II, Acquisition Category III, and Army special interest programs

(3) T&E WIPT member organizations can reverse their concurrence within the designated review period by providing written notice of nonconcurrence signed by senior management. The notice is to be sent to the PM.

(4) The approval page format is shown in appendix C, figure C–6.

i. TEMP staffing for non-tactical C4/IT and space programs.

(1) The same TEMP staffing and approval process is followed as detailed in paragraphs 3–5*b* through 3–5*h* (except para 3–5*c*).

(2) The approval page format is similar to appendix C, figures C1–C6, with the following exceptions—

(a) For OSD T&E oversight non-tactical C4/IT and space programs, the OSD DT&E, OUSD (AT&L), Director, Defense Systems, will be replaced by the Principal Director, Deputy Assistant Secretary of Defense (Programs) Office of the ASD (C3I).

(b) For non-tactical C4/IT programs, OSD or non-OSD T&E oversight, the CBTDEV concurrence signature is replaced by the FP (that is, DCS, G–1 for personnel and ASA (ALT) ILS for logistics support related TEMPs) concurrence signature.

3–6. Test and evaluation master plan format and content

a. Army policy requires that the Defense Acquisition Guidebook TEMP format be followed. Within this format, the level of detail is unique for each program and tailoring of the contents is encouraged.

b. Specific content guidance appropriate for Army TEMP preparation is contained in appendix D, which is not intended to be inclusive, since each specific program TEMP will be different based upon program's unique T&E characteristics and requirements. Guidance for ACAT II and III programs is the same as for ACAT I, except as noted. Exception: At the end of each section, where guidance on content differs for non-tactical C4/IT TEMPs, only that which is different is displayed.

c. Approval page formats and layouts for programs by ACAT are provided in appendix C.

d. An example of a T&E WIPT coordination sheet is at figure 3–7. The T&E WIPT Coordination Sheet should depict the specific participants of a program. For example, the T&E WIPT chair should show the PM and the program name; the specific school or center should be identified as the CBTDEV; and so forth.

e. Per AR 73–1, each TEMP will include a requirements/test crosswalk matrix as Attachment 1. (See para D–6 and an example at fig D–2.)

T&E WIPT COORDINATION SHEET FOR THE
TEST AND EVALUATION MASTER PLAN (TEMP) FOR
OH-42X HELICOPTER TEMP

	SIGNATURE	**DATE**
Program Manager (PMO Aviation)	*Bruce Bones* LTC Bruce Bones	Concur/~~Non-concur~~ *10 Jan 02*
Combat Developer (TRADOC Proponent school)	*J.T. Thurston* Mr. J.T. Thurston	Concur/~~Non-concur~~ *10/1/02*
System Evaluator (ATEC-AEC)	*Roscoe P. Coltrain* MAJ Roscoe P. Coltraine	Concur/~~Non-concur~~ *10 Jan 02*
Developmental Tester (ATEC-DTC/SMDC)	*Johanna Klingman* Johanna Klingman	Concur/~~Non-concur~~ *10/1/02*
Operational Tester (ATEC-OTC)	*Buster Rhymes* CPT Buster Rhymes	Concur/~~Non-concur~~ *10 Jan 02*
Logistics Analyst (ATEC-AEC-ILS)	*Freddie L. Hill* Freddie L. Hill	Concur/~~Non-concur~~ *15/1/02*
Survivability/ Lethality (ARL-SLAD)	*Edward J. Brennan IV* Edward J. Brennan IV	Concur/~~Non-concur~~ *10/1/02*
System Trainer (TRADOC)	*Russell E. Poindexter* Russell E. Poindexter	Concur/~~Non-concur~~ *16/1/02*
Threat Integrator (USASMDC - Intel)	*Roger P. Dodger* Roger P. Dodger	Concur/~~Non-concur~~ *17/1/02*

Figure 3–7. Sample test and evaluation working-level integrated product team coordination sheet

HQDA Representatives:

ASA(ALT)	Monica A. Friend Monica A Friend	Concur/~~Non-concur~~ 10/1/02
CIO/G-6	Thomas J. Loper MAJ Thomas J. Loper	Concur/~~Non-concur~~ 10 Jan 02
DUSA(OR)	Philip D. Salvo LTC Philip D. Salvo	Concur/~~Non-concur~~ 22 Jan 02
DCS, G-3	Irving R. Pilot LTC Irving R. Pilot	Concur/~~Non-concur~~ 10 Jan 02
DCS, G-8	Roger R. Wordsworth MAJ Roger R. Wordsworth	Concur/~~Non-concur~~ 10 Jan 02
Independent Logistician ASA(ALT) ILS	Katherine Beans MAJ Katherine Beans	Concur/~~Non-concur~~ 10 Jan 02
DCS, G-1	Rodney R. Rodneck MAJ Rodney R. Rodneck	Concur/~~Non-concur~~ 10 Jan 02
DCS, G-2	Thomas M. Cowan MAJ Thomas M. Cowan	Concur/~~Non-concur~~ 10 Jan 02

Others as needed:

Other Services: OTAs

Other Service User's Representatives

Associate Members (as necessary):

(examples)

Target Provider (USASMDC) (Targets PO)	John F. Cann	Concur/~~Non-concur~~ 10/1/02
Flight Test Range (USAKA Dir.)	Joyce Wilhelm	Concur/~~Non-concur~~ 10/1/02

Figure 3–7. Sample test and evaluation working-level integrated product team coordination sheet—Continued

Chapter 4
Critical Operational Issues and Criteria

4–1. Critical operational issues and criteria overview

This chapter provides content and processing guidance for development and approval of COIC during systems acquisition, modification, and upgrade.

a. Philosophy. COIC are those decision maker key operational concerns, with bottom line standards of performance that, if satisfied, signify the system is operationally ready to proceed beyond the FRP DR. COIC are not pass/fail absolutes but are showstoppers such that a system falling short of the criteria should not proceed beyond FRP DR unless convincing evidence of its operational effectiveness, suitability, and survivability is provided to the decision makers. COIC are few in number, reflect total operational system concerns, consider system maturity, and employ higher order measures.

b. Role of critical operational issues and criteria.

(1) Focus and support milestone decisions. COIC prescribe (and provide a consistent primary emphasis on) the user's minimum operational expectations for the total operational system for a favorable decision at the FRP DR. (See fig 4–1.)

(2) Reduce the multitude of operational considerations to a few operationally significant and relevant mission focused issues and criteria. Based on this mission focused nature, a system, evolutionary increment, or developmental modification that satisfies the COIC is considered by the user to be the minimum operational capability necessary (that is, just good enough) to move into production and fielding while improvement toward ORD thresholds and the full operational capability continues.

(3) Serve as umbrella issues and criteria that inherently cover a system's minimum needs for operational effectiveness, suitability, and survivability without specifically addressing these categories. The COIC are relevant to both the critical mission operations and the FRP DR. COIC integrate operational mandates with maturity considerations for the total operational system.

(4) Serve to focus and prioritize the system evaluation effort, to identify operational priorities for the acquisition effort, and to foster a coordinated effort by the members of the acquisition team by identifying and understanding what is operationally important.

(5) Apply to system evaluation. COIC are not limited to operational test (OT) issues and criteria. Being operationally relevant measures, COIC must lend themselves to assessment based on OT, DT, or other applicable methods. Data to answer the COIC can come from any credible source (for example, IOT, other OT, DT, field data collection, and studies/simulations). The system evaluator, in coordination with the T&E WIPT, develops the T&E strategy and the need for OT as well as other data sources to satisfactorily resolve the COIC. The T&E strategy is then documented in the TEMP and SEP.

c. Applicability of critical operational issues and criteria. The COIC apply to all systems (irrespective of ACAT level) during acquisition and developmental modification. During systems acquisition, the initial system will have a set of COIC applicable to the FRP DR. Each follow-on increment, if an evolutionary acquisition strategy is pursued, will have a set of COIC. COIC apply to all acquisition strategies—developmental, non-developmental, and commercial items, to include commercial-off-the-shelf (COTS). Developmental modifications are modifications that respond to preplanned product improvements identified in the original ORD or to new/revised requirements incorporated through ORD revisions. COIC supporting evolutionary acquisition and developmental modifications represent revision or refinement to the original set of COIC. Revision or refinement of COIC is not required for other system changes, such as verification of fixes to system shortcomings identified for corrections during FRP DR, PDSS, and/or routine engineering changes supporting production. In contrast to PDSS, Post production software support (PPSS) applies only to system software support for those systems that have transitioned to sustainment and the Depot Maintenance OP–29 process.

d. Focus and timing of critical operational issues and criteria. COIC are prepared and approved for inclusion in the initial TEMP for program initiation (MS B). These early COIC are based on the mission needs analysis, MNS, requirements analysis, initial ORD, and analysis of alternatives (AoA) with other documentation when needed. The COIC are updated and approved based on the updated ORD and AoA for inclusion in the TEMP approved for MS C, if conducted. COIC continually focus on the FRP decision; therefore, revision subsequent to MS C should only be necessary for significant program redirection, evolutionary increments, preplanned product improvements, and other modifications or upgrades responding to a new or revised ORD. The issues will be based on the Mission Needs Analysis and, when one exists, the MNS should remain stable during the acquisition process. The criteria reflect the maturity of the operational requirements in the ORD and AoA; therefore, they may be "soft" (that is, preliminary) initially (MS B TEMP) but will be "firm" (that is, final) standards of performance for the MS C TEMP. Performance exit

criteria with appropriate operational considerations may be used to guide the intermediate milestone decisions (for example, MS B and C). Such exit criteria will be documented in the TEMP but not as part of the COIC. The majority of performance exit criteria should be relevant to achievement of the COIC. (See fig 4–1.)

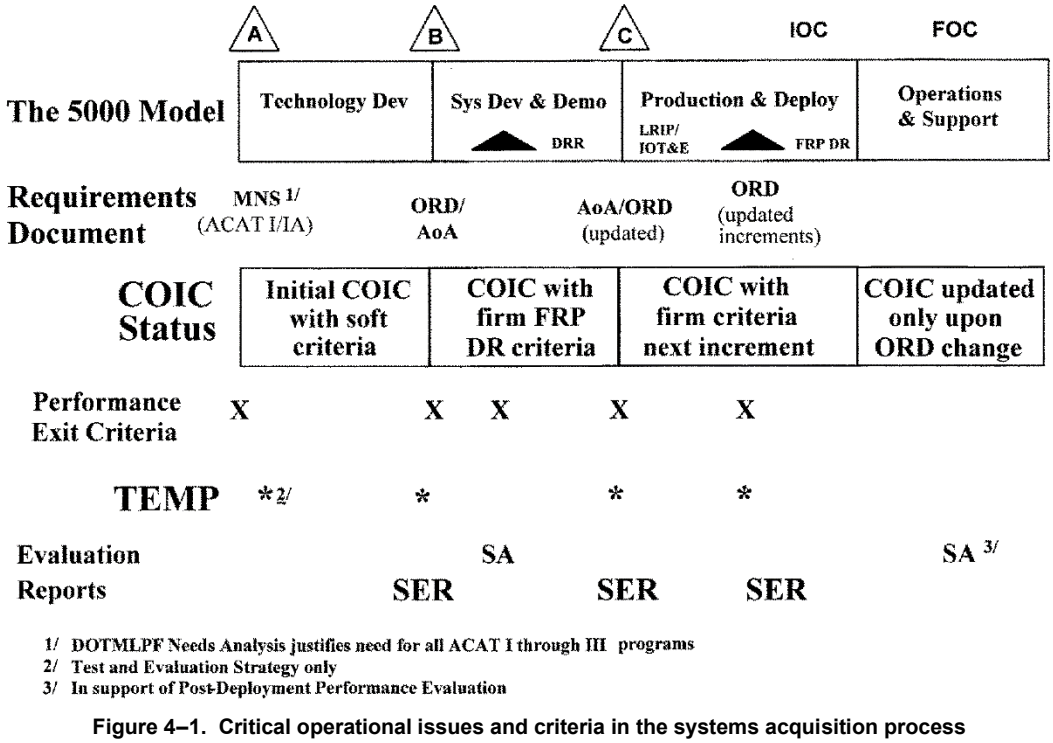


Figure 4–1. Critical operational issues and criteria in the systems acquisition process

e. Structure of critical operational issues and criteria. COIC are prepared in sets, centered on critical operational issues. For each issue, a scope, appropriate criteria, rationale for each criterion, and a set of applicable notes are developed.

(1) *Critical operational issue.* A key operational concern, expressed as a question that, when answered completely and affirmatively signifies that a system, an evolutionary increment, or a developmental modification is operationally ready to transition at the FRP DR.

(2) *Scope for the issue.* A statement of the operational capabilities, definitions, and conditions that focus the issue and guide its evaluation.

(3) *Criteria for the issue.* Those standards of operational performance that, when all are achieved, signify that the issue has been satisfied. Criteria constitute showstoppers until convincing evidence of the system's operational effectiveness, suitability, and survivability is demonstrated. Each ORD KPP will be a criterion. Criteria are not limited to only KPP.

(4) *Rationale for the criteria.* Basis for criteria and an audit trail of their link to the ORD and the AoA.

(5) *Notes for the critical operational issues and criteria.* Both mandatory and system peculiar notes apply. The mandatory notes are modified to be appropriate for the system.

f. Characteristics of a good set of critical operational issues and criteria.

(1) Operationally relevant, mission focused issues and criteria.
(2) Overarching, total operational system measures.
(3) Include all system KPPs.
(4) No overlap or duplication among criteria.
(5) Few issues and criteria.
(6) Clearly reflect why the system is being acquired.
(7) Criteria are true operational "showstoppers."
(8) Criteria are achievable and can be evaluated.

(9) Provide clear guidance on conditions applicable to measuring each criterion and for scoring the results. Avoid terms that could be misinterpreted by the organization doing the analysis and/or the evaluation.

(10) Reflect the minimal system acceptable performance for entry into FRP.

g. Team effort. Army leadership and decision makers want COIC that correctly identify and define the key operational concerns applicable to the FRP DR with true operational showstopper criteria that are achievable before and verifiable during the system evaluation in support of the FRP DR. This brings with it specific areas of focus within the roles of the CBTDEV or FP, PM or MATDEV, and system evaluator during development, coordination, and approval processing of COIC. This team functions as a subgroup of the integrated concept team (ICT) responsible for the ORD development. It is incumbent upon the CBTDEV or FP, MATDEV or PM, and system evaluator to keep their respective leadership informed of the COIC content and status during development and approval so as to ensure their concerns and guidance are addressed and problems are identified and resolved early.

(1) The CBTDEV or FP has the lead for this effort and is specifically responsible for the operational relevance of the COIC (that is, correct issues, applicable operational conditions/scope, and true operational FRP showstoppers). The CBTDEV or FP also must ensure that any doctrine (including TTP), training, leader developments, organization, and Soldier products for the system can be developed and sufficiently matured for evaluation with the materiel provided by the PM or MATDEV. The CBTDEV or FP will have to coordinate with the respective developers of doctrine, training, and organizations in scheduling and developing their products.

(2) The PM or MATDEV is responsible for assuring that the technical feasibility of the program (including the system development contract) is able to deliver materiel (for example, hardware, software, and logistics) for evaluation capable of satisfying the criteria. If this is unachievable, the PM or MATDEV advises the CBTDEV or FP and system evaluator during development of the COIC. The inability to deliver a system capable of satisfying the criteria is a condition for PM or MATDEV nonconcurrence with the COIC during coordination and processing.

(3) System evaluator determines if the COIC can be answered and provides concepts and plans for answering them. The system evaluator will coordinate with developmental and operational testers, M&S organizations, and training exercise organizations, as applicable. In some cases, these organizations may need to participate in the COIC development. Inability to answer an issue or verify achievement of one or more criteria is a condition for evaluator nonconcurrence during coordination and approval processing of the COIC.

4–2. Critical operational issues and criteria relationships

COIC are derived from documented operational requirements to reflect those minimum essential operational concerns and operational performance standards essential to FRP authorization. Accordingly, COIC development relies upon many activities and documents associated with requirements determination and definition, system acquisition, and system fielding. COIC serve as a primary focus for the system evaluation supporting the FRP DR to aid in the overall evaluation of the system's operational effectiveness, suitability, and survivability, as well as identification of improvements needed. Inherently, the COIC serve to guide the acquisition and development effort by identifying those system operational performance capabilities and standards that the user representative (that is, CBTDEV or FP, as applicable) considers most important. These relationships are depicted in figure 4–2.

a. Critical operational issues and criteria and operational requirements. Operational requirements, along with key employment considerations, are essential to establishing operationally valid, relevant, and credible COIC. The operational requirement is reflected in the Mission Needs Analysis, MNS, Requirements Analysis, ORD, and AoA.

(1) *Critical operational issues and criteria and operational requirements documents.* The critical operational issues will be based on the MNS (or the Mission Needs Analysis when MNS is not produced) and thus unlikely to change as the program proceeds. The criteria will be based on the ORD, along with the associated Requirements Analysis, and, thus, change as the requirements mature. This does not mean that issues and criteria should always be direct lifts from these documents; rather there should be a clear, auditable foundation for the issues and criteria in these documents. For example, the ORD may require a significant survivability improvement over the existing system, whereas the AoA and cost considerations may result in a criterion to complete 20 percent more missions with 50 percent more threats neutralized. The rationale for COIC provides a crosswalk between the ORD minimum acceptable requirements and the criteria. While the COIC development for an existing system may rely on a validated ORD, COIC development for future systems should occur concurrently with the ORD development.

(a) Critical operational issues and criteria and operational requirements document key performance parameter. All KPP are included as criteria and are direct lifts from the ORD. KPP are by definition FRP DR "showstoppers." Figure 4–3 depicts the salient characteristics of KPP and COIC. Additionally, each KPP must be clear, measurable, testable, and achievable. When writing the ORD KPP, the ORD developer tailors a set of KPP that serve as criteria for the COIC, thus, simplifying the acquisition process by providing a single requirement document (that is, the ORD) and COIC development/approval to mostly extraction from the ORD.

(b) Critical operational issues and criteria and other operational requirements document requirements. When the existing ORD does not include KPP that provide a complete set of overarching requirements reflecting a good enough system for entry into FRP, the other ORD requirements serve as a basis for development of the criteria. Often the ORD rationale statement is a better source for COIC requirements than the actual requirements because they may be more overarching and operational in focus. Additionally, the AoA, specifications, experiments, and study results may have to be used in conjunction with the ORD criteria to develop COIC. Also, the ORD requirements should be assessed in the system evaluation per the Defense Acquisition Guidebook. The other ORD requirements serve to identify satisfactory achievements that do not need further attention as well as specific shortcomings that need improvement as the system moves into FRP and fielding.

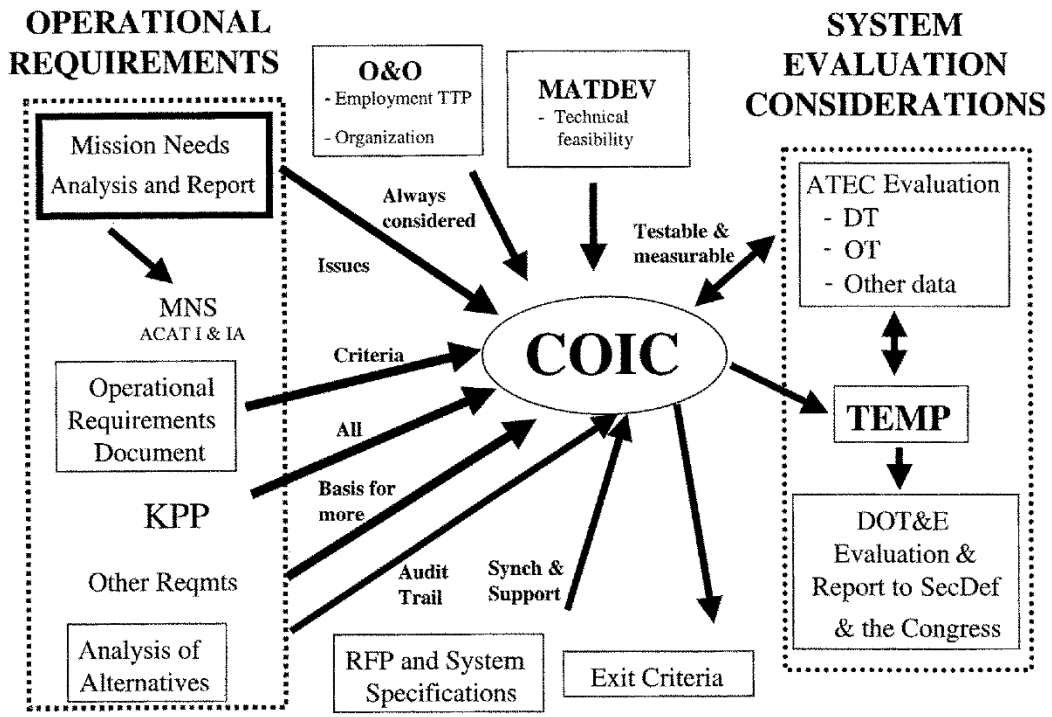


Figure 4–2. Critical operational issues and criteria relationships

(2) *Critical operational issues and criteria and analysis of alternatives.* The AoA is the primary analytical document of operational consideration during MS B decisions. It compares the relative cost and operational effectiveness for alternative concepts considered and indicates their relative status to the baseline. As such, it represents significant expectations for the concept chosen to proceed. For instance, if the AoA shows a significant cost savings over the baseline and this is the purpose of the acquisition (modernization), then the criteria should reflect a system that is as mission capable, trainable, and sustainable in combat as the existing system. The AoA uses various MOPs that aid in establishing criteria for the COIC. Because of the significance of the AoA to the program, there must be an audit trail of consideration among the COIC, ORD, and AoA. The Defense Acquisition Guidebook encourages linkage between MOE/MOS (AoA and system evaluation plan), system requirements (ORD and specifications), and T&E (COIC and CTP) for ACAT I and IA programs. This linkage allows for evaluation of whether the system remains cost and operationally effective when performance shortfalls are found during T&E. The COIC will have an audit-trail to the AoA where possible and be identified in the rationale.

b. Critical operational issues and criteria and system specifications. The primary objective is compatibility between the COIC and the System Specifications (or contract represented by the specifications). The MATDEV or PM assures this compatibility and advises the CBTDEV and system evaluator when an incompatibility exists. If an incompatibility exists, then the ORD takes precedence or an Army leadership decision is needed. Incompatibility represents a serious situation in that the contract will be insufficient to allow the system to fulfill the minimum user needs, thus jeopardizing a successful FRP DR. Occasionally the specifications include operational performance parameters

based upon specific features that were not included in the ORD, but affect the criteria. Changes to the ORD and/or System Specifications may occur as a result of the COIC development and approval process.

c. Critical operational issues and criteria and other requirements documents (studies and cost). When the MNS/ORD, AoA, and System Specifications do not provide all requirements information needed to develop a valid set of COIC, other sources (such as studies, experiments, and cost analyses) are addressed. Most of the time, these sources are considered in establishing MNS/ORD requirements (for example, operation and support costs are used to establish reliability and maintainability requirements considered during COIC development).

d. Critical operational issues and criteria and operational employment considerations. To produce operationally realistic and valid COIC, the COIC must focus on the critical operational missions assigned to the system, its organization, system employment TTP, and leadership implications. An understanding of how the system fights, operates, and functions is critical to determining if system or organizational-type measures should apply (for example, a system that fights as an element of a platoon, with target detection and hand-off for engagement accomplished internal to the platoon, should not be measured as a single, stand-alone system but as a platoon). Similarly, an understanding of how system operations will be logistically supported is essential in defining sustainment COIC. Operational requirements must, therefore, be examined in light of operational employment considerations to arrive at meaningful criteria for COIC. Also, the employment conditions or constraints (for example, day, night, limited visibility, specific battlefield conditions, critical payloads, line of sight, non-line of sight, and queuing) must be addressed in either the scope or criteria of the COIC.

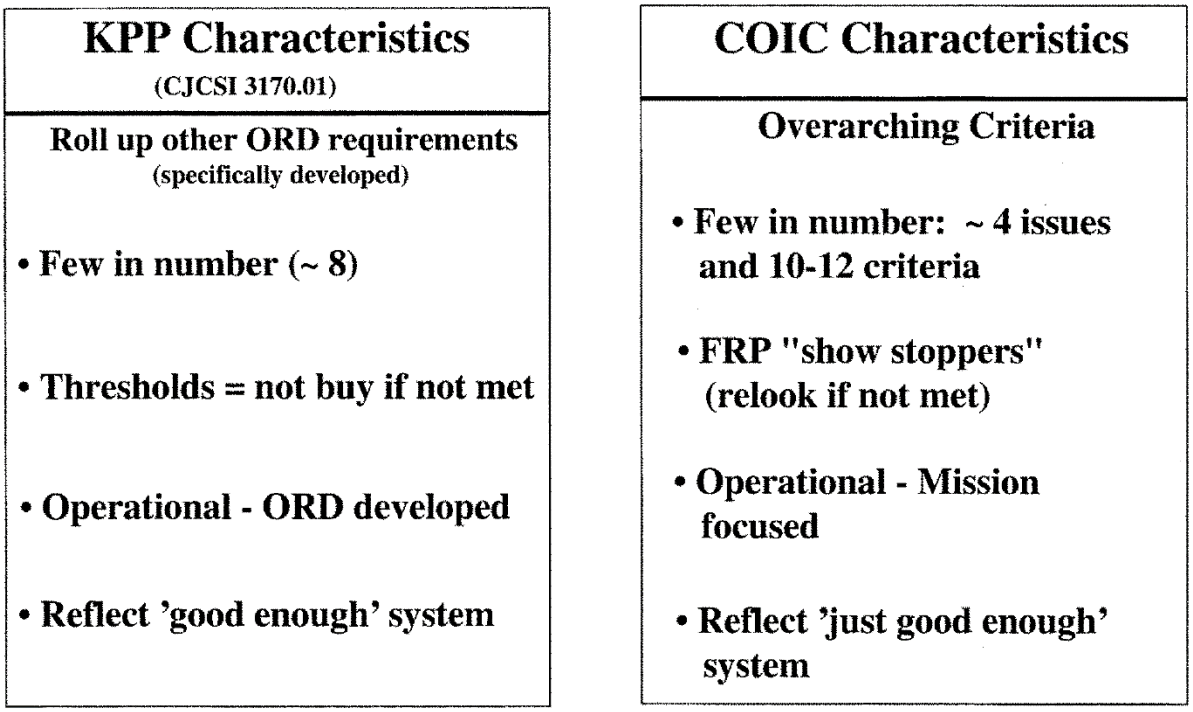


Figure 4–3. Key performance parameter–critical operational issues and criteria relationship

e. Critical operational issues and criteria and performance exit criteria. Criteria, by definition, are bottom line standards that, if satisfied, indicate that a system is operationally ready to proceed at the FRP DR. Performance exit criteria, meanwhile, are established in accordance with DoDI 5000.02 and the Defense Acquisition Guidebook at each milestone for the next milestone and for major events between milestones. While documented in the TEMP, such exit criteria will not be part of the COIC. The majority of the performance exit criteria should be relevant to achievement of the criteria. They are minimum requirements that must be successfully demonstrated for the program to proceed to the next acquisition milestone. Performance exit criteria, as such, serve as decision point measures of progress, or "steppingstones" toward achievement of COIC and eventually, the mature system's objective performance. While the CBTDEV has the lead in developing the COIC, the PM or MATDEV has the lead in developing exit criteria and does

so with the assistance of the CBTDEV in coordination with the system evaluator. When separate MS C and FRP DR criteria exist, MS C performance exit criteria will normally measure technology maturity and the feasibility of fulfilling operational needs/requirements and readiness for the system to begin LRIP. The FRP performance exit criteria and COIC will focus on a mission capable, supportable, and life-cycle affordable system. The relationship of COIC and performance exit criteria, from MS B to FRP DR, is depicted in figure 4–4.

f. Critical operational issues and criteria and the system evaluation. The system evaluator is responsible for planning a complete and comprehensive system evaluation that—

(1) Provides an independent evaluation or assessment of system operational effectiveness, suitability, and survivability as well as the system's ability to perform its operational missions in the expected operational environment. This includes development of AI so as to fully address operational effectiveness, suitability, and survivability (see chap 5) and being able to indicate or isolate the cause of operational shortfalls whenever possible.

(2) Provides timely advice to PM or MATDEV and CBTDEV or FP on the progress of their respective components of the system toward achievement of the COIC and AI during the system's acquisition process. Such assessments allow these developers to adjust their program to provide needed corrective actions early in the system's acquisition process.

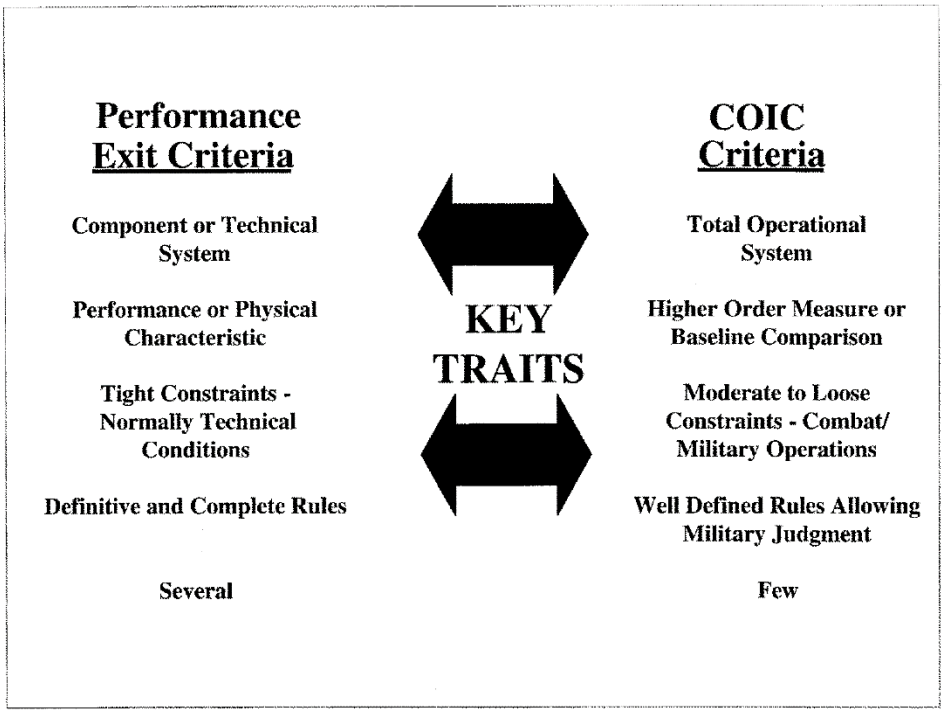


Figure 4–4. Relationship of critical operational issues and criteria and performance exit criteria

(3) Answers the COIC for the FRP DR. Any source of data (for example, operational test, developmental test, study, experiments, and/or surveys) judged credible by the system evaluator can be used to answer the COIC. The SER reports the system's achievement against the COIC and AI and must be clearly articulated for decision makers and action officers. However, the system evaluation reporting for the FRP DR is not limited to only the COIC assessment. The system evaluator must clearly describe the evaluation approach. The system evaluator also provides interim assessments of the status and risks for achievement of the COIC leading up to the FRP DR, particularly in the case of a MS C (LRIP decision). Plans and reports for system evaluations after the FRP DR will use these same COIC, unless evolutionary acquisition, Pre-planned Product Improvement (P3I), or a revised ORD apply to the evaluation and the operational requirements demand change in the COIC (for example, new or revised KPP). The COIC are first documented in the TEMP prior to MS B to influence the program and evaluation planning and conduct leading to MS C.

(4) Determines whether the ORD requirements have been satisfied.

g. Critical operational issues and criteria and system evaluation measures. Chapter 5 discusses the system evaluation measures in further detail. COIC are an essential element to formulate a comprehensive evaluation strategy.

(1) To plan and accomplish the system evaluation, the evaluator prepares a comprehensive and definitive set of MOPs, MOEs, and MOSs from both the operational and technical perspectives. The COI and AI are the evaluation issues for which the system evaluator defines measures. The generation of these measures gives the system evaluator an enormous amount of latitude with regard to the scope and focus of the system evaluation. However, inappropriate measures may result in unnecessary, increased T&E resource requirements or in misleading the acquisition community and decision makers. Informal, early coordination of the evaluation measures with the CBTDEV or FP and MATDEV or PM should be the norm for the system evaluator and should be sought by the CBTDEV or FP and PM or MATDEV to avoid major problems late in the program (for example, during the SEP development).

(2) Although the focus of COIC is the minimum system operational capabilities needed (that is, what is operationally good enough) for a go-ahead decision at the FRP DR, system evaluation measures focus on a complete and comprehensive evaluation of the system's operational effectiveness, suitability, and survivability. The SERs whether the system can perform (effective, suitable, and survivable) all missions and attempts to isolate cause of problems when possible (see figs 4–5 and 4–6).

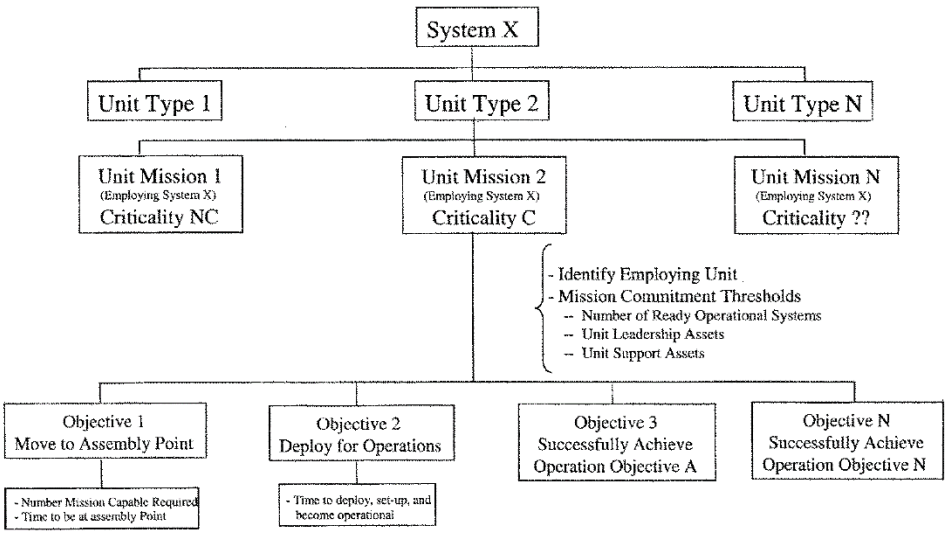


Figure 4–5. Critical operational issues and criteria mission capability dendritic

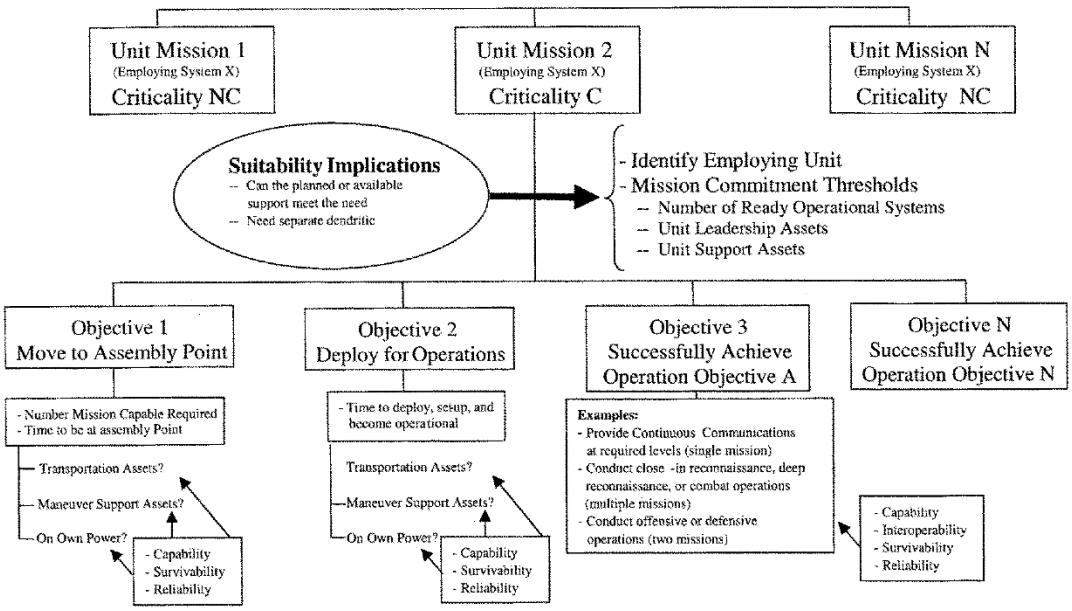


Figure 4–6. System evaluation mission capability dendritic

(3) System evaluation measures support or complement COIC resolution as follows (see fig 4–7):

(a) Allow the system evaluator to specify the data required from multiple sources for COIC not directly answerable from a single data source. For testers, analysts, and system evaluator execution purposes, these measures are just as critical as the COIC they support. If the data are not provided, the system evaluator will not be able to evaluate the issues for the FRP DR.

(b) Provide the system evaluator the diagnostics to identify factors contributing to or causing a performance shortfall for one or more of the COIC.

(c) Complement the COIC by providing a comprehensive evaluation of all aspects of the total operational system. In the event of a performance shortfall for one or more COIC, the evaluation measures may provide the evidence needed to convince decision makers that the system is good enough to proceed (for example, baseline comparison or accomplishment of specific ORD thresholds inherently covered within an overarching COIC). Even when the COIC are satisfied, the evaluation measures normally identify areas for continued improvement as the system proceeds in acquisition (for example, fixes for shortfalls against ORD thresholds or where continued effort toward ORD objective values has significant operational benefit). The system evaluation may also serve to identify a measure of critical importance that was not identified during the COIC development process.

4–3. Development and approval processes for critical operational issues and criteria

a. Appendix E provides detailed COIC format and content guidance.

b. Figure 4–8 depicts an overview of the COIC process. Appendix F provides detailed COIC process guidance for materiel, tactical C4I/IT, and non-tactical C4/IT programs.

(1) COIC Development Concurrent with the ORD. COIC are initially developed with the ORD and refined with the ORD. The CBTDEV has the lead for the ORD and COIC development processes for materiel and tactical C4/IT programs. The FP has the lead for the ORD and COIC development processes for non-tactical C4/IT programs.

(2) Coordinating Draft COIC with major Army command (MACOM) headquarters, T&E WIPT, and AoA organization. Per figure 4–8, the draft COIC are readied for and begin coordination while the ORD is in staffing. While the CBTDEV or FP has the lead for the documents being coordinated, it is a team effort with the MATDEV or PM and system evaluator. The T&E WIPT uses the initial COIC to build the draft TEMP. Subsequent refined versions of the COIC are included in the TEMP until the ORD and COIC are approved, at which point the TEMP is readied for approval.

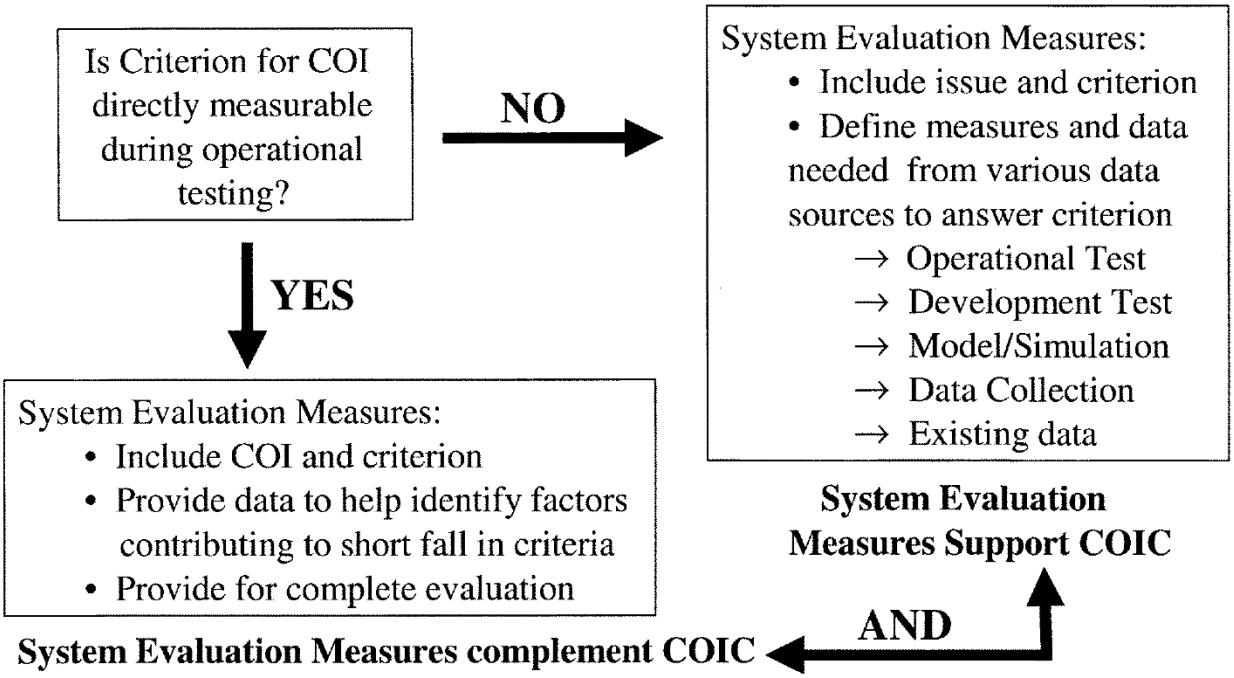


Figure 4–7. Critical operational issues and criteria relationship to system evaluation measures

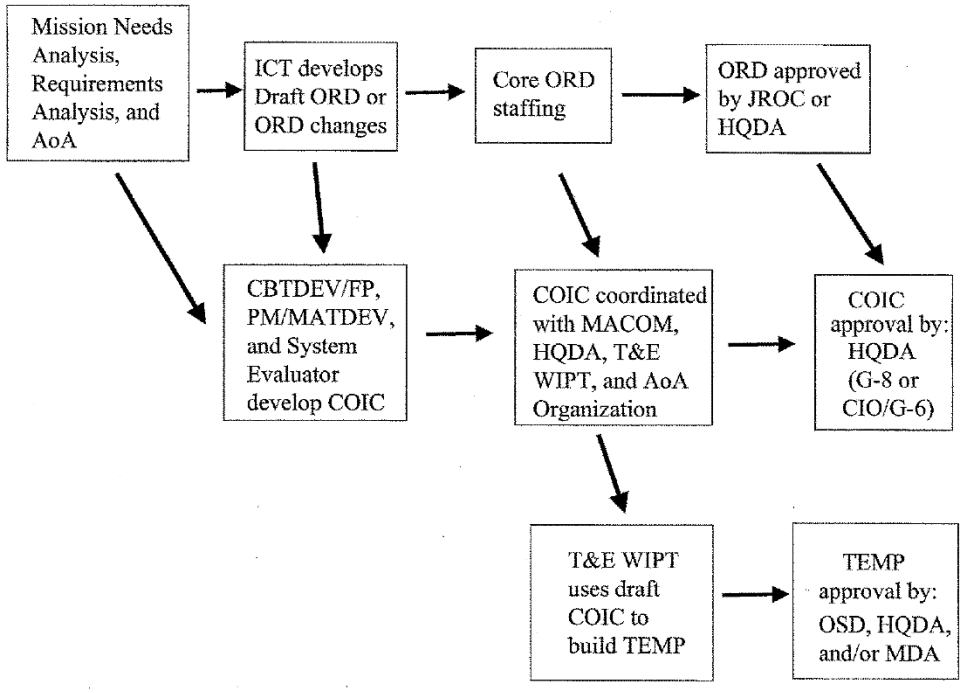


Figure 4–8. Critical operational issues and criteria process overview

(3) Similar to the ORD approval, HQDA approves all COIC. For materiel and tactical C4I/IT programs, the DCS, G–8 approves the COIC. CIO/G–6 approves all non-tactical C4/IT program COIC. An ORD that includes a synopsis of the analysis results must be approved before COIC can be approved. The ORD–COIC "Crosswalk" Matrix (see fig 4–9) is a key element during the COIC approval process at HQDA (that is, DCS, G–8 and CIO/G–6). The matrix is encouraged for use during proponent reviews as well. Additionally, the matrix will be the basis for the mandatory Attachment 1 to the TEMP (that is, Requirements/Test Crosswalk Matrix). (See para 3–6*e* and fig D–2.)

4–4. Critical operational issues and criteria–operational requirements document–test and evaluation master plan schedule synchronization

A synchronized schedule among the ORD, COIC, and TEMP, as well as other events during a system's acquisition is critical to avoid delays in the TEMP approval process. The "long pole" in the process is ORD approval, especially when HQDA and JROC approvals are required as shown in figure 4–10. Detailed schedule planning factors and critical events for synchronization are provided at appendix F.

4–5. Critical operational issues and criteria approval guidelines and staffing considerations

a. Table 4–1 identifies the COIC approval authorities.

Table 4–1
Critical operational issues and criteria approval authorities

Program type	Approval authority	Package address
ACAT I and ACAT IA (Tactical)	DCS, G–8 (Director, Force Development)	THRU: CG, ATEC FOR: HQDA, ATTN: DAPR–FDR
ACAT IA (Non-Tactical) and all Non-Tactical C4/IT with OSD or HQDA T&E Oversight	CIO/G–6 (general officer)	THRU: CG, ATEC FOR: HQDA, ATTN: SAIS–ION
ACAT II and III Materiel and Tactical C4I/IT ACAT II and III Non-Tactical C4/IT without OSD or HQDA T&E oversight	DCS, G–8 (Director, Force Development) CIO/G–6 Colonel or civilian equivalent	THRU: CG, ATEC FOR HQDA, ATTN: DAPR–FDR FOR: HQDA, ATTN: SAIS–ION

b. A team effort among the CBTDEV or FP, PM or MATDEV, and system evaluator is imperative and is reflected in the COIC process by the requirement for the CBTDEV or FP to obtain command positions from PM or MATDEV and ATEC before submission to HQDA for approval. PM or MATDEV should nonconcur if the capabilities or performance required by the COIC are not technically feasible or achievable by the FRP DR. ATEC should nonconcur if the capability or performance required by the COIC cannot be evaluated by the FRP DR. Both cases preempt the FRP decision because capabilities that the user representative says must be present to enter FRP either cannot be delivered or confirmed. In the case of OSD T&E Oversight programs, DOT&E will report to the Congress the inability to satisfy the mission need as an ineffective or unsuitable system for FRP, unless some convincing evidence is presented before the DOT&E beyond low-rate initial production (BLRIP) report is rendered. Avoid setting firm criteria too early (for example, Milestone B) if the FRP decision is to follow Milestone C. Approval of the firm COIC may be completed in support of a TEMP update between Milestone B and C. This strengthens CBTDEV or FP credibility by allowing time for the requirement to mature and program to stabilize.

c. COIC staffing and approval submission packages are described below.

(1) *Materiel and Tactical C4I/IT Programs.* The staffing and approval package consists of a cover memorandum, the proposed draft COIC (fig E–2), and the ORD–COIC crosswalk matrix (fig 4–9). The CBTDEV proponent submits the COIC package to the MACOM headquarters. The MACOM staffs the COIC with the PM or MATDEV and ATEC for their command positions and submits them through the Commanding General (CG), ATEC to DCS, G–8 for approval. Sample memoranda for the CBTDEV proponent COIC submission, MACOM headquarters staffing with the PM or MATDEV and ATEC, and MACOM headquarters COIC submission to DCS, G–8 are at appendix F. Throughout the process both hard copy documents and electronic files are passed in order to speed the process.

(2) *Non-Tactical C4/IT Programs.* The staffing and approval package consists of a cover memorandum, the proposed draft COIC (fig E–2), and the ORD–COIC crosswalk matrix (fig 4–9). The FP submits the COIC package to the MACOM. The MACOM staffs the COIC with PM or MATDEV and ATEC and submits them through CG, ATEC to the CIO/G–6 for approval. Sample cover memoranda for the FP COIC submission, MACOM headquarters staffing with PM or MATDEV and ATEC, and MACOM headquarters COIC submission to the CIO/G–6 are in appendix F.

SAMPLE ORD-COIC CROSSWALK

Medical Communications for Combat Casualty Care (MC4) System

ORD Reference (*indicates a KPP)	Critical Operational Issues and Criteria
Supports the requirement that the Service supplied computer hardware used to run the TMIP software must meet the minimum hardware requirements stated in the TMIP TEMP. 1.f. (2) (a), page 10: The MC4 program will "develop the Army's infrastructure for the utilization of the Joint TMIP software." 4.a (2), page 28: The MC4 system has the mission to "provide the computer infrastructure for the Army's implementation of the Joint TMIP software. As needed, development software for Army-unique medical requirements not met by TMIP." *4.b (2) (a) i, page 31: The MC4 computer hardware must be able to run the operating system utilized by TMIP.	1.2.1.2 The MC4 computers must provide significant processor speed and memory capacity to run the TMIP software. 1.2.1.3 Any MC4 supplied software must be compatible with the TMIP software.

Figure 4–9. Sample operational requirements document–critical operational issues and criteria crosswalk matrix

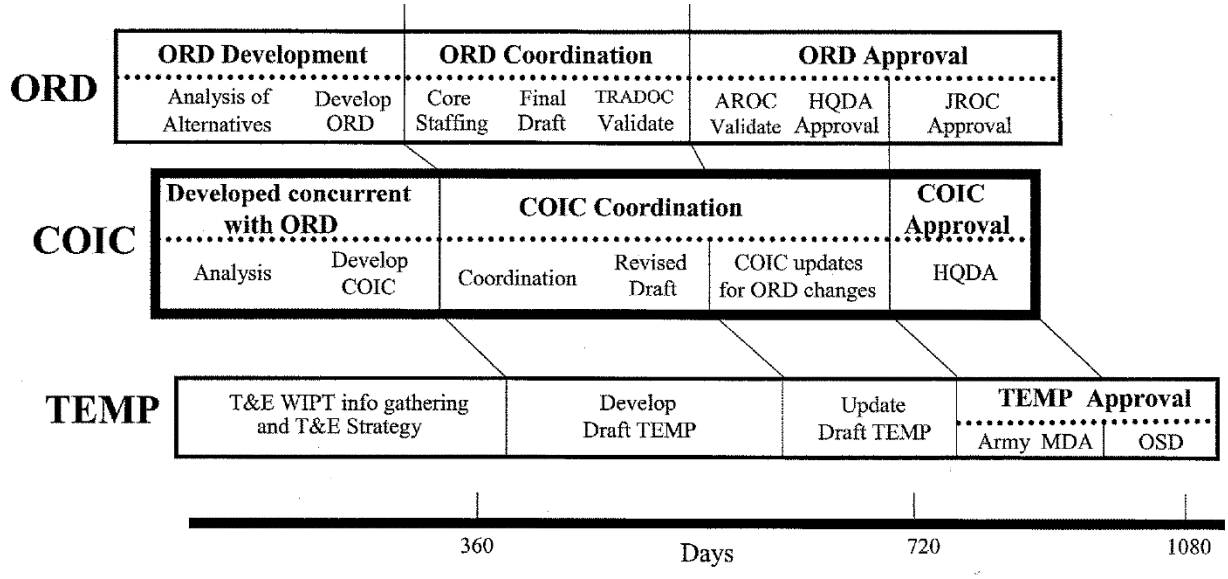


Figure 4–10. Time synchronization of operational requirements document, critical operational issues and criteria, and test and evaluation master plan

d. Approval memorandum requirements follow.

(1) *Materiel and Tactical C4I/IT Programs.* COIC for materiel and tactical C4I/IT programs are approved by the HQDA Director, Force Development, G–8 and forwarded to the applicable PM or MATDEV for inclusion in the

TEMP with copies furnished the CBTDEV proponent, MACOM headquarters, and Army Evaluation Center (AEC). Samples of COIC cover memoranda are at appendix F.

(2) *Non-Tactical C4/IT Programs.* COIC for non-tactical C4/IT programs are approved by the CIO/G–6. Either a general officer or colonel (or civilian equivalent) approves the COIC depending on whether OSD or HQDA T&E oversight applies. The CIO/G–6 COIC approval authority forwards the approved COIC to the PM or MATDEV for inclusion in the TEMP with copies furnished the FP, MACOM headquarters, and AEC. Samples of COIC approval memoranda are at appendix F.

4–6. Critical operational issues and criteria update considerations

a. Update between MS B and C for the initial FRP DR. COIC are updated as a program proceeds through the acquisition process and as the ORD progresses in its development and approval. COIC are initially developed for the TEMP supporting MS B with "soft" criteria reflecting the lack of maturity in the ORD requirement. The COIC supporting the TEMP for MS C will have firm criteria. If there is no MS C, the ORD and COIC must be finalized sufficiently in advance of IOT (or other testing/data gathering events supporting the FRP DR) to allow for TEMP update and approval in advance of IOT.

b. Update in support of TEMP revision supporting the FRP DR. Only update the COIC for the FRP DR when there are ORD capabilities still to be delivered (that is, future evolutionary acquisition increments and preplanned product improvement set forth in the ORD) and the effort is being approved by the FRP DR. Generally, firm criteria should only be provided for the next increment capability with soft criteria (or to be determined notes) applicable to criteria for future increments. Revised COIC are not needed to support follow-on testing beyond the FRP DR if correction of shortcomings do not require future minimum user needs (that is, operational efficiency and user preference for system increases as performance improves).

c. Update after FRP DR. There are two reasons for updating the COIC after the FRP DR—

(1) The COIC were incorrect and change was identified during the T&E process and FRP DR.

(2) An ORD change is occurring requiring additional capabilities. If the T&E process and FRP DR determined that one or more criteria were not met at the FRP DR, then the criteria must be deleted or added to future increments. The complete rationale must be provided justifying inappropriate use of the criteria as a showstopper for the FRP decision and the course of action recommended. The rationale for such change should have been documented in the system evaluation and/or FRP acquisition decision memorandum. Administrative changes to the ORD do not require COIC changes. After the FRP DR, the COIC will change only when new capabilities are added that add to, or change, or existing showstopper requirements.

4–7. Critical operational issues and criteria checklist

A COIC checklist is provided at appendix G for use in preparation, review, and processing of COIC. The checklist addresses both content and processing of COIC.

4–8. Critical operational issues and criteria development example

Appendix H contains a COIC development example using a plausible situation and providing a school solution.

4–9. Critical operational issues and criteria procedures for joint and multi-Service programs

COIC apply to joint and multi-Service programs whether the Army is the lead or a participating Service. Either total program or Army-only COIC will be developed, approved, and included in the TEMP. Guidance of this pamphlet applies regarding content, focus, and Army approval processing of COIC. Army participants in joint and multi-Service programs will familiarize other Service participants with the Army COIC procedures, because COIC are peculiar to the Army. The T&E WIPT for a joint program may decide to apply Army COIC guidance and build COIC for the TEMP in which case the Army COIC will be embedded in the overall set of program COIC. When the Army is lead for a joint or multi-Service program, a single integrated set of COIC will be developed and approved for inclusion in the TEMP. Army COIC approval procedures will be as set forth in this pamphlet. Other Services will be responsible for approval processing of the COIC within their respective Services. For those programs where the Army is a participant (that is, not the lead Service), Army COIC will be developed, approved, and included in the TEMP as an appendix. The issues should be those COIs determined by the program T&E WIPT for inclusion in Part IV of the TEMP that are applicable to the Army. The nature of joint and multi-Service programs often leads to compromises regarding certain required capabilities in order to acquire a system useable by all involved Services. Criteria will reflect these compromises. MATDEVs and system evaluators must continue their respective roles, addressed above, in order for the criteria to be realistically achievable and evaluated. Other Service representatives must understand the serious implications of these activities relative to FRP DR, particularly when a system is on the OSD T&E Oversight List.

Chapter 5
System Evaluation

Section I

Introduction

5–1. Overview of system evaluation

Conducted by the system evaluator, the system evaluation is a program level analytical process that supports the systems acquisition process and provides information to the CBTDEVs and MATDEVs, decision makers, and other members of the acquisition team on the status of the system. System evaluation begins as early as possible in the life cycle of a system (for example, as early as the battlefield functional mission area analysis for materiel systems and the information management plan for IT systems). Evaluation continues through the system's post-deployment activities.

a. CE is the approach used to implement system evaluation. CE is conducted throughout the systems acquisition process. It emphasizes the role of the system evaluator and ensures a responsible, timely, and effective assessment of the progress toward a mature system.

b. CE may produce a SA (as necessary) at specific points to assess technical risks, address performance and support requirements, assess potential operational effectiveness, suitability, and survivability, examine logistic and training supportability, support the type classification and materiel release, and determine interoperability with other Army systems, other U.S. Services, North Atlantic Treaty Organization (NATO), and other allies' systems.

c. At each milestone DR (except MS A) and the FRP DR, the system evaluation process produces a SER that focuses on the system's progress toward satisfying the threshold or objective requirements (for example, the COIC); provides demonstrated operational effectiveness, suitability, and survivability; identifies acquisition and operational risks; and recommends future courses of actions for the MATDEV or PM and CBTDEV.

d. Early involvement of the system evaluator in the acquisition process, vis-à-vis the ICT, is vital to a successful systems acquisition program. This early involvement ensures appropriate data are available to support the system evaluation objectives, and that all credible data and resources are used effectively and efficiently. The system evaluator works closely with the analytical, test, and training communities, MATDEV, and CBTDEV to ensure that explicit and implicit system evaluation requirements placed on these organizations are clearly understood and are obtained in a timely and efficient manner in support of the system evaluation.

5–2. Scope of system evaluation

System evaluation encompasses a broad analytical approach to the evaluation of an acquisition program from earliest concept definition through post deployment and sustainment. A continuous approach to system evaluation has evolved to include examination of developmental, production, and post-fielding system effectiveness to provide extensive coverage of acquisition events. A CE approach requires the system evaluator to—

a. Identify the specific mission tasks and system functional capability to be studied and evaluated over the acquisition life cycle.

b. Consider the physical, military, and civilian environments to be encountered by the acquisition system.

c. Determine the events, to include the system and mission-level measurements and data requirements necessary to verify the adequacy of system attributes (for example, mission and technical performance, training, RAM, tactics, logistics support, and software) and to determine the accomplishment of mission-level tasks.

d. Require timely execution of such events to ensure technical and operational readiness for IOT, when conducted.

e. Monitor the events and assess the adequacy of the system with respect to its stated requirements.

f. Monitor the corrections applied and assess the adequacy of the corrective actions to the identified deficiencies.

g. Periodically report on the status of the system with respect to its technical and operational attributes to the CBTDEV, TNGDEV, or FP; MATDEV or PM; and milestone decision principals, as appropriate.

5–3. Objectives of system evaluation

The major objective of the system evaluation is to address the demonstrated system effectiveness, suitability, and survivability of Army and multi-Service systems for use by typical users in realistic operational environments. During development, the system evaluation provides developers and decision makers with a comprehensive assessment of a system's ability to meet the stated need in its current state of development and estimates the potential for a successful, mature configuration. Ultimately, it provides an evaluation of how the system performed with respect to its intended mission in its intended environment based on the system requirements. Other system evaluation objectives are—

a. Determine the degree to which the critical operational issues have been addressed.

b. Discover critical problems, either technical or operational, at the earliest opportunity so that they may be addressed and resolved by either the CBTDEV or FP or MATDEV or PM before they affect major decisions.

c. Support the formulation of realistic system operational requirements and technical specifications and ensure they are measurable and testable.

d. Provide for early and frequent assessment and reporting of a system's status during development.

e. Compare system development efforts against existing DoD mandates to determine scope of compliance (that is, Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP), JTA, and Common Operating Environment) as well as any potential compliance migration efforts, especially during PPSS and PDSS.

f. Support having operationally effective, suitable, and survivable systems transition from development into production.

g. Reduce test time and cost through comparison analyses, data sharing, and use of all credible data sources (such as M&S).

h. As required, provide assessments of system capabilities and burdens after deployment.

5–4. System evaluation in support of systems acquisition and development

The emphasis of the system evaluation, and its supporting testing, changes as the system moves through design and engineering toward a fully mature system ready for fielding. This section provides information on the types of evaluation and the data sources needed in each phase of the systems acquisition process. This guidance is provided for those systems that are entering the acquisition model at MS A; however, the flexibility of the model allows each program to adapt these guidelines as appropriate. A SER is required at each MS decision (except MS A) and the FRP DR. SAs are prepared at other decision points or as requested.

a. Systems acquisition overview (see para 1–5).

(1) Acquisition strategies. The acquisition strategy defines how the program is structured to achieve full capability. AR 70–1, Army Acquisition Policy, identifies two approaches: evolutionary and single step to full capability. The approach to be followed depends on the availability of time-phased requirements in the ORD, the maturity of technologies, the relative costs and benefits of executing the program in blocks versus a single step, including consideration of how best to support each increment when fielded. The rationale for choosing one of these approaches will be addressed in the acquisition strategy.

(2) Spiral development. Either acquisition approach (that is, evolutionary or single step) involves an iterative process for developing a set of operational capabilities known as spiral development. In this process, the requirements are refined through experimentation and risk management, there is continuous feedback, and the user is provided the best possible operational capability. The spiral development process provides an opportunity for interaction between the user, tester, and developer. Spiral development, including software, implements evolutionary acquisition.

(3) Evolutionary acquisition. The evolutionary acquisition strategy is the preferred approach to satisfying operational needs. Evolutionary acquisition strategies define, develop, and produce/deploy an initial, militarily useful capability ("increment I") based on proven technology, time-phased requirements, projected threat assessments, and demonstrated manufacturing capabilities and plan for subsequent development and production/deployment of increments beyond the initial capability over time (increments II, III, and beyond). The scope, performance capabilities, and timing of subsequent increments are based on continuous communications among the requirements, acquisition, intelligence, and budget communities. In planning evolutionary acquisition strategies, PMs are required to strike an appropriate balance among key factors, including the urgency of the operational requirement; the maturity of critical technologies; and the interoperability, supportability, and affordability of alternative acquisition solutions.

(a) Evolutionary acquisition is an approach that fields an operationally useful and supportable capability in as short a time as possible. This approach is particularly useful if software is a key component of the system and is required for the system to achieve its intended mission. Evolutionary acquisition delivers an initial capability with the explicit intent of delivering improved or updated capabilities in the future.

(b) In an evolutionary approach, the ultimate capability delivered to the user is divided into two or more increments, with increasing levels of capability. Deliveries for each increment may extend over months or years. Increment I provides the initial deployment capability (a usable increment of capability called for in the ORD). There are two approaches to treatment of subsequent increments—

1. The ORD includes a firm definition of full operational capability, as well as a firm definition of requirements to be satisfied by each increment, including an initial operational capability (IOC) date for each increment. In this case, each increment is baselined and the acquisition strategy defines each increment of capability and how it will be funded, developed, tested, produced, and operationally supported.

2. The ORD includes a firm definition of the first increment but does not allocate to specific subsequent increments the remaining requirements that must be met to achieve full capability. In an evolutionary acquisition, the specific requirements for increment I are defined in the ORD, based on the user's increased understanding of the delivered capability, the evolving threat, and available technology, lead-time-away from beginning work on increment II, and so on, until full capability is achieved. Requirements that cannot be fulfilled during a specific increment development, with the approval of the requirements authority, may be delayed to the next increment development. The first increment, and each subsequent increment, is baselined in conjunction with the MDA authorizing work to proceed on that increment. The acquisition strategy defines the first increment of capability; how it will be funded, developed, tested, produced, and supported, the full operational capability the evolutionary acquisition is intended to satisfy; and the funding and schedule planned to achieve the full operational capability to the extent it can be described. The strategy also defines the management approach to be used to define the requirements for each subsequent increment and the acquisition strategy applicable to each increment, including whether end items delivered under earlier increments will be retrofitted with later increment improvements.

(4) When a program has time-phased requirements and utilizes an evolutionary acquisition strategy, each increment has a set of parameters with thresholds and objectives specific to the increment. Each increment requires an independent system evaluation to support decision makers.

(5) The T&E strategy for a program using an evolutionary acquisition strategy will remain consistent with the time-phased requirements in the ORD, acquisition strategy, and APB. Planning for T&E will acknowledge the increment deliveries established in the acquisition strategy and baselined in the APB. The evaluation concept will be specific to each increment of the militarily useful capability planned.

b. System evaluation activities during the technology development phase. In this phase, the most promising system concepts are defined in broad objectives for cost, schedule, performance, software requirements, opportunities for tradeoffs, overall acquisition strategy, and T&E strategy. The CBTDEV prepares an ORD, which is derived from the Mission Needs Analysis, Requirements Analysis, Analysis of Alternatives, STRAP, and the STAR. An ORD includes KPP and other operational capability requirements. The CBTDEV develops the COIC, while the MATDEV or PM develops the CTPs.

(1) During this phase, the system evaluation usually is in support of defining materiel concept solutions to satisfy the materiel need identified in the mission needs analysis, that is, the development of concepts of materiel, doctrine, training, leadership, and organization tied to the identified materiel solution. The CBTDEV, with support from ATEC or SMDC, may utilize the Battle Labs to execute warfighting experiments including CEPs and advanced warfighting experiments (AWEs) to aid in defining operational requirements that may also support the system evaluation. The CEP and AWE allow the CBTDEV to examine and resolve combat development, materiel concept, doctrinal, leadership, organization, and training issues. In support of a concept study, a technical feasibility test (TFT) or early user test (EUT) may be conducted to determine safety and feasibility of the components/subsystems if a concept has been chosen. (See chap 6.)

(2) When a program has been established, the T&E WIPT will craft a T&E strategy to support preacquisition and early acquisition process activities. The T&E strategy will address live testing and M&S, recognizing the respective risks, to evaluate system concepts against mission requirements. Consistent with the T&E strategy, the system evaluator will develop a SEP. If a MS A occurs, the initial SEP will be the evaluation strategy. A SER is prepared to support approval of a new acquisition program at MS B.

(3) Application of M&S in this phase focuses on the mission need. Simulation can be used to demonstrate military utility of new tactics, technologies, and systems as well as to provide insights into human/machine interaction requirements. Engineering level models of new designs can provide estimates of system and subsystem performance to support higher level models such as engagement/combat models. If engineering level models are not yet available, reasoned representations of the desired system could be used in combat models to assess potential battlefield contribution and to formulate basic estimates of the KPPs and COI criteria required. An AoA is conducted during this phase and assesses relative cost and effectiveness of the alternative concepts.

(4) Specific evaluation activities conducted during the technology development phase may consist of the following—

(a) Participating in the ICT that develops the ORD.
(b) Participating in the T&E WIPT.
(c) Participating in the AoA efforts.
(d) Supporting the initial COIC development and approval process.
(e) Assisting in developing system characteristics and exit criteria.
(f) Developing the initial SEP consistent with the acquisition strategy.
(g) Participating in development, staffing, and approval of the TEMP.

(h) Identifying all required tests events, M&S activities, and other data collection events.

(i) Developing a SER in support of MS B and a SA at other times, when requested.

(j) For those weapons systems required by law to undergo LFT&E, develop a live fire strategy (see app J).

c. System evaluation activities during the system development and demonstration phase. Approval at MS B establishes a new acquisition program and concept baseline to include authorization for entry into the system development and demonstration phase.

(1) The key objective of this phase is to demonstrate that the technologies critical to the most promising concept can be incorporated into the system design.

(2) Tests conducted in this phase include an engineering DT (EDT) of prototypes, critical systems, subsystems, and components, contractor tests, EUT, limited user test (LUT), AWE, and Joint Warfighter Interoperability Demonstration. An EDT assists in identifying and reducing design risk and indicates the degree to which new or emerging technologies pose a risk to the program. A production prove-out test may be conducted at the subsystem level to provide data on safety, achievability of technical parameters, and determination of technical risks. An EUT assesses the degree to which the selected design approach will operate in the intended operational environment. A LUT may be conducted to obtain data to support the system evaluation required for a LRIP decision. T&E will also be conducted to address doctrine, training, organization, leader development, materiel requirements, and logistics support aspects of the system, using surrogate systems if necessary. The use of M&S is strongly recommended in this phase to aid in the system evaluation. The system evaluation will address realistic program performance and suitability thresholds. See chapter 6 for a detailed discussion of testing.

(3) Simulation-based testing techniques can be applied to digital product descriptions, system models, and hardware components, to predict system performance in support of early feasibility tests and design trade-off analyses. Human-in-the-loop (HITL) simulators enable Soldiers to interact with early system models. Computer generated test scenarios and forces, as well as synthetic stimulation of the system, can support system evaluation and testing by creating and enhancing realistic live test environments. Test results provide data for validation of system models and digital product descriptions, while M&S can identify and help resolve issues of high technical risk, requiring more focused testing. The system evaluator uses models to predict performance in areas that are impractical or impossible to test.

(4) Specific evaluation activities conducted during the system development and demonstration phase may consist of—

(a) Continued participation in the T&E WIPT.

(b) Supporting the COIC update and approval process.

(c) Supporting the ORD update and approval process.

(d) Participating in the update, staffing, and approval of the TEMP.

(e) Supporting AoA update efforts.

(f) Assisting in the development of exit criteria.

(g) Updating the SEP, as appropriate.

(h) Participating in the simulation support plan (SSP) update.

(i) Planning all required data sources (for example, tests, M&S, and market surveys).

(j) Providing evaluation status at TRRs, as appropriate.

(k) Developing a SER in support of a MS C, if conducted.

(l) Developing a SA to support intermediate DRs, when required.

d. System evaluation activities during production and deployment prior to the FRP. When conducted, MS C authorizes entry into LRIP and continuation into the production and deployment phase. The key objective of this phase is to achieve an operational capability that satisfies mission needs.

(1) During this phase, the system (including necessary training devices, threat simulators, test equipment, and computer resources) is engineered, integrated, tested, and evaluated to ensure the—

(a) System design is stable.

(b) System meets contract specifications and technical parameters.

(c) System is operationally effective, suitable, and survivable in its operational environment.

(d) System meets minimum essential user requirements.

(e) System is ready for production.

(f) System is supportable.

(g) System is ready for materiel release and deployment.

(2) Testing is conducted on prototype, production-representative, or production systems. Both DTs and OTs are conducted during this phase. A production qualification test (PQT), conducted at system level using LRIP items if available, provides data on the reduction of design risks, achievement of the CTPs, contractual compliance, the type

classification determination, and validation of general and detailed specifications, standards, and drawings for use in production. The system design must be sufficiently mature to provide adequate support packages for testing and to ensure that the system is representative of the production system to enable valid assessments of the system. A LUT may be conducted to assess risk for selected operational requirements. LRIP items are delivered for use in the IOT that, for ACAT I and II programs, must be conducted prior to the FRP DR. See chapter 6 for a detailed discussion on testing.

(3) During this phase, a comprehensive full-up, system level (FUSL) LFT&E is required on covered systems before the FRP DR. See appendix J for a detailed discussion of the LFT&E strategy and document requirements.

(4) The iterative use of M&S and T&E supports the overall design and evolutionary development of a system. T&E uses M&S tools to provide mechanisms for planning, rehearsing, optimizing, and executing complex tests. The virtual proving ground (VPG) and other M&S capabilities provide synthetic environments and stimuli for more controllable, repeatable testing of system models and hardware throughout the acquisition cycle. Integration of simulation and testing provides a means for examining why the results of a physical test might deviate from pre-test predictions. Integrating M&S with testing also generates significantly more understanding of the interaction of the system with its environment than either M&S or testing alone.

(5) Specific evaluation activities conducted during the production and deployment phase prior to the FRP DR may consist of—

(a) Continued participation in the T&E WIPT.

(b) Continued support to the COIC update and approval process for future increments.

(c) Supporting the ORD update and approval process, if appropriate.

(d) Participating in the update, staffing, and approval of the TEMP.

(e) Supporting AoA update efforts, if conducted.

(f) Assisting in the development of exit criteria, if appropriate.

(g) Updating the SEP.

(h) Participating in the SSP update.

(i) Planning all required tests, M&S activities, and other data collection events.

(j) Providing evaluation status at TRRs, as appropriate.

(k) Developing a SER in support of the FRP DR.

(l) Developing a SA to support intermediate DRs, when required.

e. System evaluation activities during FRP and deployment. A favorable FRP DR represents approval to build the total expected buy (that is, to enter the FRP and deployment phase), to materiel release the system, to deploy/field the system, and to support the system while authorizing entry into the operations and support phase. The key objectives of this phase are to verify that the production item meets CTPs and contract specifications, determine the adequacy and timeliness of any corrective actions indicated by previous tests, and ensure that the item continues to meet operational needs.

(1) System evaluation is an integral part of the acceptance and introduction of system changes to improve the system, react to new threats, and reduce life-cycle costs. Production verification test (PVT) are system-level tests conducted to verify that the production item meets CTPs and contract specifications, to determine the adequacy and timelines of any corrective action indicated by previous tests, and to validate manufacturer's facilities, procedures, and processes. A PVT will also provide a baseline for the test requirements In the technical data package for post-production testing. A follow-on operational test (FOT) may be necessary during or after production to refine the estimates made during IOT, provide data to assess changes, and verify that deficiencies in materiel, training, or concepts have been corrected. See chapter 6 for a detailed discussion on testing.

(2) Specific evaluation activities conducted during the FRP and deployment phase may consist of—

(a) Continued participation in the T&E WIPT.

(b) Planning all required tests.

(c) Providing evaluation status at TRRs, as appropriate.

(d) Participating in the SSP update.

(e) Developing a SER, when requested.

(f) Developing a SA to support reviews (that is, materiel release).

f. System evaluation activities during the operations and support phase. The objectives of this phase are to execute a support program that meets operational support performance requirements and sustainment of systems in the most cost-effective manner. The sustainment program includes all elements necessary to maintain the readiness and operational capability of deployed systems. A SA may be developed as necessary to address changes that occur during this phase, such as minor modifications and reprocurements as well as newly mandated DoD requirements.

g. System evaluation activities during evolutionary acquisition after the FRP decision. The system reenters the acquisition process at MS B for development of the subsequent increments. The program is defined in the acquisition strategy, APB, and TEMP at the FRP DR.

5–5. System evaluation in support of other than new systems acquisition and development

a. System evaluation in support of system changes. See AR 750–10. A system change is a modification or upgrade to an existing system. It can be an alteration, conversion, or modernization of an end item that changes or improves the system's capabilities or fixes corrections to deficiencies after the FRP DR. For purposes of this document, the term "modification" will be used when the system is still in production and an "upgrade" will be used when the system is out of production (see AR 73–1). T&E is conducted to ensure that the modification or upgrade achieves the desired effect based upon performance, reliability, safety, or system logistical characteristics.

(1) *Modifications.* Any modification that is of sufficient cost and complexity that it could qualify as a MDAP or MAIS will be a considered for management purposes as a separate acquisition effort. Modifications that do not cross the MDAP or MAIS threshold will be considered part of the program being modified (original program), if the program is still in production. If the program is out of production, the modification will be considered a separate acquisition effort. In either case, all modifications must undergo a system evaluation and most will require some level of testing to gather the requisite data.

(a) The T&E strategy for a modification will vary depending on whether the modification is considered to have significant operational impact, some operational impact, or no operational impact. The CBTDEV or FP is responsible for determining whether a system change has operational impact, in consultation with the MATDEV or PM and system evaluator. The checklist at figure 5–1 will aid in determining which operational impact classification applies. For those modifications with operational impact, the system evaluator must draw upon military expertise, system acquisition knowledge, and current Army policy when developing the T&E strategy in consultation with the T&E WIPT.

(b) A modification that is in response to a new or revised operational requirement or that is intended to fill an existing operational requirement is considered to have significant operational impact. For materiel systems, this would normally result in the development of a T&E strategy, formation of a T&E WIPT, and update to the system TEMP.

(c) A modification that has some operational impact typically impacts mission logistics. Such modifications require a T&E strategy developed within the T&E WIPT even though the system change does not respond to an existing or updated operational requirement.

(d) If a modification has no operational impact, then the procuring command will determine the T&E actions necessary to support the decision. Such modifications do not respond to existing or changing operational requirements.

(e) As a general rule, the system evaluation will require testing. If there is any modification in the operational performance envelope, the system evaluation may require both DT and OT. If there is no operational impact, normally DT data will satisfy the system evaluator's needs. The T&E requirements are developed in coordination with the T&E WIPT and documented in the system's TEMP.

(2) *Upgrades.* In an evolutionary acquisition, the ultimate capability delivered to the user is divided into two or more increments, with increasing increments of capability. Increment I provides the initial deployment capability (a usable capability called for in the ORD). The ORD includes a firm definition of initial and full operational capability, as well as a firm definition of time-phased requirements to be satisfied by each increment. The T&E strategy must address the requirements for each increment. Upgrades, when planned or known, should be identified in the TEMP.

b. System evaluation in support of commercial items and non-developmental items. Commercial items and non-developmental items (NDIs) provide a preferred alternative to a full system developmental program. If the market surveillance reveals an item that has a high probability of meeting the user's requirements and is cost effective across the life cycle, the potential item is investigated. Depending on the item's technical maturity and its ability to satisfy stated entrance criteria (such as minimum accomplishments required to be completed prior to entry into the next phase), the commercial item or NDI may enter system acquisition at the FRP DR.

(1) Commercial item and NDI categories. There are two general categories of commercial items and NDIs and a third level of effort not designated as a separate category.

(a) A commercial item and NDI that fully meet the user's needs without modification may enter the acquisition model during the production and deployment phase. The FRP DR verifies the sufficiency of the item against the requirement and initiates type classification with reduced milestone decision documentation. This category consists of off-the-shelf items (for example, commercial, foreign, or other Services) that will be used in the same environment for which they were designed and will require no modification.

(b) A commercial item or NDI requiring minor modification to an off-the-shelf item may involve an abbreviated system development and demonstration phase to address necessary modifications. Here, limited testing may be required to verify the impact of the modifications on performance and reliability. This approach may require a MS C

decision to enter into production or procurement if the system is a non-major program that does not require LRIP. This category consists of off-the-shelf items to be used in an environment different from that for which designed or that requires military ruggedization.

(c) The integration of a commercial item and/or NDI components into larger parent systems, both developmental and non-developmental is encouraged. The integration of commercial item or NDI components and systems resulting in a new system can be designated as a commercial item or NDI, as applicable. This category is focused on integration or assemblage of existing proven commercial components (commercial part integration).

(2) Consideration standard. To be considered as commercial item or NDI, any integration effort should involve only minor modifications to each commercial item or NDI component or subsystem to achieve successful integration. When pursued as a commercial item or NDI strategy, integration of components and subsystems requires an early and realistic assessment of the size of the integration effort and the associated risks. Because commercial items and NDI integration results in an essentially new system, focused risk management is essential throughout the acquisition process and increased requirements for T&E over the more classic forms of commercial items and NDIs are involved.

(3) Market surveys and investigations. Market investigations in support of commercial components/items may require a system evaluation, possibly with appropriate testing, to support development and updates to the system specification. The MATDEV involves the system evaluator in the development of the survey/investigation questionnaire to ensure that all required data are collected.

(4) Steps leading to the SER for commercial items and NDIs. A T&E WIPT is formed, a TEMP developed, and system evaluations are conducted. Each system evaluation makes maximum use of all existing data (including M&S, results of market surveys/investigations, and contractor data). The system evaluation must address the same issues as would be addressed for a full developmental program. A SEP is prepared to document specific data requirements and sources. Testing may be required to verify achievement of CTPs and operational effectiveness, suitability, and survivability. A SER will be developed to support the acquisition decision.

SYSTEM CHANGE CLASSIFICATION CHECKLIST

1. IS THIS SYSTEM CHANGE IN RESPONSE TO A NEW OR REVISED OPERATIONAL REQUIREMENT?
   IF "YES" - SYSTEM CHANGE WITH SIGNIFICANT OPERATIONAL IMPACT
   IF "NO" - GO TO QUESTION 2

2. IS THE SYSTEM CHANGE AN ADDITIONAL BLOCK IN AN EVOLUTIONARY ACQUISITION APPROACH LISTED IN THE CURRENT APPROVED ACQUISITION STRATEGY FOR THE PURPOSE OF ACHIEVING EXISTING OPERATIONAL REQUIREMENTS?
   IF "YES" - SYSTEM CHANGE WITH SIGNIFICANT OPERATIONAL IMPACT
   IF "NO" - GO TO QUESTION 3

3. DOES THIS SYSTEM CHANGE AFFECT SYSTEM OPERATIONAL CHARACTERISTICS, PERFORMANCE OR TACTICAL EMPLOYMENT, AND LOGISTICS SUPPORT BY THE USER?
   IF "YES" OR "NOT SURE" - GO TO QUESTION 3A
   IF "NO" - SYSTEM HAS NO OPERATIONAL IMPACT
   (GO TO QUESTION 4)

3A. BASED ON COORDINATION WITH USER REPRESENTATIVE, IS A NEW OR REVISED OPERATIONAL REQUIREMENT NEEDED?
   IF "YES" - SYSTEM CHANGE WITH SIGNIFICANT OPERATIONAL IMPACT
   IF "NO" - GO TO QUESTION 3B

3B. BASED ON COORDINATION WITH USER REPRESENTATIVE, DOES THE SYSTEM CHANGE HAVE OPERATIONAL IMPACT?
   IF "YES" - SYSTEM CHANGE WITH OPERATIONAL IMPACT
   IF "NO" - SYSTEM HAS NO OPERATIONAL IMPACT
   (GO TO QUESTION 4)

4. DOES THIS SYSTEM CHANGE SIGNIFICANTLY ALTER THE CONFIGURATION OF THE SYSTEM OR END ITEM IN ANY OF THE FOLLOWING AREAS?
   - TECHNICAL MANUALS
   - TMDE OR TEST PROGRAM SETS
   - SPECIAL TOOL SETS
   - TRAINING AND TRAINING DEVICES
   - RAM CHARACTERISTICS
   - TECHNICAL SURVIVABILITY, VULNERABILITY, OR LETHALITY CHARACTERISTICS
   - HUMAN FACTORS OR SAFETY CHARACTERISTICS
   - NEW OR NOT FULLY DEVELOPED TECHNOLOGY EMPLOYED
   - INTEROPERABILITY
   - MULTISERVICE IMPACT

   IF "YES" - SYSTEM WITH SIGNIFICANT TECHNICAL CHANGE
   IF "NO" - SYSTEM WITH OTHER TECHNICAL CHANGES ONLY

Figure 5–1. System change classification checklist

c. System evaluation in support of reprocurements. See AR 73–1 and DA Pam 70–3. Reprocurement of an item is authorized when a continuing need based on an existing or updated performance specification or purchase description from the last procurement has been identified and validated by the CBTDEV. If it is determined that a change in the ORD requirements is needed, the program will be treated like a system change program from a system evaluation standpoint. If the results of the review indicate that no change in the ORD requirements is warranted, the required evaluation and supporting test events can be greatly simplified. In this case, the PVT normally satisfies the system evaluation requirements to ensure compliance with the specification.

(1) System evaluation requirements vary depending on the degree of configuration stability and whether the reprocurement is—

(a) A commercial item, NDI, or a military standard item (a Government controlled technical data package).

(b) An item from a contractor different from the original item contractor.

(c) An item with a significant break in procurement (more than 2 years).

(2) System evaluation (including an analysis of logistics and training impact) may be required to support a MS decision if market investigations reveal that a commercial item previously procured is no longer available and significant configuration changes or technology advances have occurred that may result in a new acquisition strategy. Market investigations supporting such reprocurements may include necessary testing to support updates to the system specifications.

d. A system evaluation strategy should be developed to support Army experiments and demonstrations. See AR 73–1. These are pre-acquisition efforts that may allow accelerated entry into the systems acquisition process.

(1) *Advanced technology demonstrations.* Advanced technology demonstrations (ATDs) allow the warfighter to explore military utility, affordability, and potential of technologies to support warfighting concepts.

(a) The evaluation strategy for an ATD will include experiments, demonstrations, and tests, as appropriate, documented using the TEMP format, tailored as appropriate.

(b) Formal T&E WIPTs are not required. The T&E documents do not require formal staffing or approval and are maintained by the program sponsor.

(c) System acquisition programs with approved TEMPs that have been redesignated as an ATD will continue to maintain TEMPs. The TEMP will reside and be maintained by the MATDEV. If a program is directed to reenter the formal acquisition process, the MATDEV will follow the formal policy and procedures in obtaining TEMP approval by the appropriate approval authority (see chap 3).

(2) *Advanced concept technology demonstrations.* Advanced concept technology demonstrations (ACTDs) are sponsored by OSD. Being user oriented and dominated, ACTDs provide a mechanism for intense involvement of the warfighter while incorporation of technology into a warfighting system is still at the informal stage.

(a) The system evaluation strategy for an ACTD will include experiments, demonstrations, and tests, as appropriate, documented using the TEMP format. Formal T&E WIPTs are not required. The T&E documents do not require formal staffing or approval and are maintained by the program sponsor.

(b) System acquisition programs with approved TEMPs that have been redesignated as an ACTD will continue to maintain TEMPs. The TEMP will reside and be maintained by the MATDEV. If a program is directed to reenter the formal systems acquisition process, the MATDEV will follow the formal policy and procedures in obtaining TEMP approval by the appropriate approval authority (see chap 3).

(3) *Warfighting experiments.* Warfighting experiments provide data and insights in support of the requirements determination process, force development process, and technology transition process. They provide information to evaluate major increases in warfighting capability. Although experiments are not designed as rigorous tests to support systems acquisition DRs, they generally contribute data to system evaluations, under CE, and should reduce the requirements for tests, especially in the early systems acquisition phases. Warfighting experiments include—

(a) Advanced warfighting experiment. A single AWE normally includes several technologies, materiel concepts, and systems in various stages of acquisition. Where possible, data collected during AWEs will be used to reduce operational test requirements.

(b) Concept experimentation program. A CEP is made up of discrete experiment events that investigate materiel concepts or warfighting ideas. Planning and execution of each CEP experiment is patterned after the T&E of systems in the acquisition model with as much scientific rigor as practical.

(4) *Force development test or experimentation.* The FDT/E supports the force development process by examining the effectiveness of existing or proposed concepts or products of doctrine, organizations, training, leadership and education, personnel, and facilities (DOTLPF). The FDT/E may be a stand-alone effort or it may be related to, or combined with, OT and should be documented in the TEMP. If conducted in lieu of an EUT, the results are included in the system evaluation. Data from the FDT/E will assist in determining essential and desirable system capabilities or characteristics. See chapter 6 for a detailed discussion on testing.

e. System evaluation in support of limited procurement. Limited procurement (LP) type classification is used when a materiel item is required for special use for a limited time. The specified limited quantity for the LP item will be procured without intent of additional procurement of the item under this classification. The LP type classification is used to meet urgent operational requirements that cannot be satisfied by an item type classified as standard.

(1) Criteria for LP type classification of an item required for urgent operational use will include the following:

(a) Existence of an urgent operational requirement substantiated by the using command representative and by the CBTDEV or HQDA.

(b) Determination that there is no type classified item that fully satisfies the requirement.

(c) Sufficient definition of the military characteristics of the item in materiel requirements documents to allow subsequent evaluation of the item.

(d) Demonstration that the proposed item does not qualify for standard type classified and offers no more than a moderate risk.

(e) Determination that the proposed item can be economically maintained and logistically supported in the geographic area and timeframe for which the type classification is valid.

(2) Type classification of LP will not be used solely to avoid the acquisition process or to avoid T&E.

(3) Not later than 6 months following delivery of the initial shipment of the LP item, the user or requester of the item will collect data and provide an operational field evaluation statement to the PM or mission assignee agency. Information copies will be provided to HQDA (ATTN: SALT–RPP), TRADOC, Army Materiel Systems Analysis Agency (AMSAA), and ATEC (AEC).

(4) System evaluation activities include—

(a) Preparing a SEP.

(b) Assisting the CBTDEV or FP in developing the ORD and COIC.

(c) Determining the need for DT, a quick reaction LUT, or other data collection events.

(d) Providing a SA to support LP type classification of the system based on program documentation, available test results, M&S, and other data collection events.

(e) Providing a SA to support materiel release under LP.

f. System evaluation in support of foreign comparative testing. The program for foreign comparative testing (FCT) generally fits into the Army acquisition cycle as part of the normal evaluation process of NDI. The FCT process is dependent on a developed foreign item, user interest, a valid requirement, good procurement potential, and a successful evaluation. (See AR 73–1.) See chapter 6 for a detailed discussion on testing.

(1) *Foreign comparative testing procedures.* After an item has met all criteria of the DoD FCT and nomination has been approved, a SEP will be prepared. Foreign and contractor data will be used to the maximum extent possible to satisfy the system evaluation requirements. If sufficient data are not available, test items will be obtained from the foreign county by way of loan, lease, or purchase, whichever is most advantageous to the Army and agreed to by the foreign country.

(2) *Foreign comparative testing reporting.* The Army FCT Executive Agent provides oversight of all FCT projects, and all plans and reports will be provided through the FCT Executive Agent.

Section II

Requirements Translation

5–6. Overview of requirements

a. The CBTDEV develops the operational requirements for new tactical systems or changes to existing tactical systems. FPs develop operational requirements for new non-tactical C4/IT systems and changes to non-tactical C4/IT systems. A system evaluation strategy development begins during the requirements development process to ensure that system requirements are stated in clear, concise, and where appropriate, measurable operational terms. For materiel and tactical C4I/IT systems, the system evaluators participate in the development of operational requirements (that is, MNS, CRD, and ORD) through ICTs (see AR 71–9). The focus of participation is understanding the need and operational requirements and ensuring the requirements stated in CRD and ORD can be evaluated and answered.

b. In order to develop a sound T&E strategy, the system evaluator and testers must ensure that inconsistencies in the specification of requirements are resolved through their review of each requirements document (for example, MNS, CRD, and ORD). This review and a review of the system specification and the RFP will determine how to best support the strategy and to justify any need for changes to milestones or events.

5–7. Translating requirements

The proper interpretation of user requirements and the subsequent translation of the broad operational capability needs into system-specific operational requirements, to system performance specifications, to evaluation issues, and then to testing issues/parameters are the first steps in developing a T&E program.

a. Development of contractual documents. The MATDEV generates the contractual documents. Because these contractual documents must be legally exacting and enforceable as well as technically complete, they are usually more voluminous and quite different from the corresponding ORD. The testers and system evaluator must be involved in the development of these documents (that is, the RFP and related contractual documents such as the system and development specifications) throughout the review process. The T&E WIPT must review section 3 of the system specifications to ensure the proper criteria are reflected and the requirements are measurable and testable. The T&E WIPT may be requested to assist in generating the test methods and procedures contained in section 4 of the system

specifications. If a Statement of Objectives is used in the RFP, then the T&E WIPT should review the contractor-generated system specification.

b. Confirmation of the transition process. When the contractor receives the contractual document containing these requirements, there is another translation process. This is the actual fabrication of an end product intended to meet not only the technically exacting specifications of the contract but also the APB requirements. Test data provide the MATDEV, the system evaluator, and the decision maker with information on the contractor's success at meeting the performance standards and establish the safety parameters for testing. In a technical sense, the process is a feedback loop that measures what was produced by the contractor against what was a requirement under the contract. This process is important because it allows the MATDEV to replicate and correct/enhance the product when problems are revealed. It also confirms that the product being produced is acceptable.

5–8. Overview of the operational requirements document

a. General description of operational capability. The general description section of the ORD identifies the statement of need, describes the overall mission area in terms of the Army Universal Task List, identifies linkages to CRD, describes the proposed system, summarizes supporting analyses, and introduces time-phased requirements so evolutionary acquisition can be applied. Perhaps the most significant of these is the Operational and Organizational Description provided in the system description. This operations oriented description links with the future concepts and defines where and how the system fits on the future battlefield and its anticipated contributions to future operations. As such the description serves as underpinning for the remainder of the ORD.

b. Capabilities required. The capabilities required section of the ORD provides the required operational capabilities, including parameters with threshold and objective values, applicable increments, and rationale for each parameter and value. Four sections of requirements apply: system performance; IERs; logistics and readiness; and environmental, safety, occupational health, and other system characteristics.

c. Key performance parameters. All system ORDs have KPPs, which are those system capabilities considered essential for mission accomplishment. There are only a few KPPs that are roll-ups of other ORD capabilities. Not achieving a KPP threshold can be cause for a concept or system to be reevaluated and a program to be reassessed or terminated (that is, a FRP decision showstopper).

d. Analysis of alternatives. The analysis of alternatives (AoA) is a rigorous, quantitative analysis, conducted by TRADOC, designed to assess multiple program alternatives along the lines of cost, operational effectiveness, and technical risk, as well as the tradeoffs between these elements. The findings from the AoA provide the analytic underpinnings for development of the ORD and refinements to the ORD KPPs. A list of supporting analyses, including AoA results, is attached to the ORD. This list includes a short description summary of the analyses used to develop the ORD and a synopsis of key pertinent results.

e. Program support, force structure, schedule, and program affordability constraint requirements. These sections of the ORD identify various system and program objectives and constraints applicable to achieving the required operational capabilities.

f. Attachments. Operational mode summary (OMS)/mission profile (MP) and the SSP are attached to the ORD.

5–9. Development of evaluation issues

a. Evaluation issues. Evaluation issues consist of the COIC, developed by the CBTDEV or FP, and the AIs, developed by the system evaluator, to ensure that a comprehensive plan for addressing a system's operational effectiveness, suitability, and survivability.

b. Critical operational issues and criteria. The COIC are derived from the operational requirement and reflect the minimum essential operational concerns and standards requiring answers during the system evaluation. Approved COIC are used to determine the scope, emphasis, and intensity of the T&E effort. This determination is the basis for the resources (such as personnel, time, facilities, equipment, instrumentation, and funds) that must be committed to obtain the data to answer the issues and evaluate the degree to which the criteria are met. Detailed guidance for preparation, coordination, and approval of the COIC statement is provided in chapter 4 and appendix E.

c. Additional issues. AIs are evaluation focus areas developed by the system evaluator to supplement and complement the COIC. They are developed for those aspects of the system not covered by the COIs. Each AI set includes statement of the issue, scope, and measures. The resources necessary to address these AIs, if additional to the resources for the COIC, should be identified in the TEMP. For a more detailed discussion of AI in system evaluation, see paragraph 5–15.

d. Measures of effectiveness and measures of performance. The COIC and AIs define high-level evaluation issues for which the system evaluator develops the MOEs and MOPs. The MOEs and MOPs are used to design test events so data collected are sufficient to address all the different ways in which a requirement may have been interpreted.

The evaluation issues and MOEs and MOPs are examined to ensure that each and every requirement is covered by a COI or AI and by a MOE and MOP. The end product is a consistent, fully justified set of evaluation issues that form the foundation for the SEP. See paragraph 5–22 for details regarding the process of developing MOEs and MOPs.

5–10. Critical technical parameters

CTPs are parameters that must be met. They are developed by the MATDEV, in conjunction with the system evaluator and CBTDEV, with input from other T&E WIPT members as required. The CTPs are listed in matrix format with accompanying objectives and thresholds in Part I of the TEMP (see app D).

a. Each CTP has measurable objectives and thresholds to be evaluated. The parameters are derived from the ORD and included in the system specifications/contract, the system characteristics (including software maturity and performance measures), and the technical performance measures. CTPs establish a relationship between the operational requirements and testing to be performed and evaluated during acquisition. CTPs are evaluated using data obtained through testing, surveys, studies, M&S, or other analytical means.

b. Part I of the TEMP includes the specific CTPs that the MDA has designated as exit criteria and that must be confirmed in each phase of testing. To ensure a smooth transition of the system to the initial operational test and evaluation (IOT&E), the CTPs should be linked to the COI (see chap 4).

c. The following areas should be considered when applicable: system performance, physical attributes, security attributes, RAM, system safety, transportability, health hazards, natural environmental or climatic effects, logistic supportability, software reliability and maintainability, compatibility and interoperability, survivability, including conventional ballistic vulnerability, nuclear hardness and survivability, electromagnetic environmental effects (E3), directed energy vulnerability, chemical, biological, radiological vulnerability, electronic warfare (EW), countermeasures, counter-countermeasures, training, vulnerability, and lethality.

d. Noncritical technical parameters are parameters that do not have to be met for a system to continue to be acquired. They are developed by the PM or MATDEV and included in the system specifications and program documentation. The system evaluator may develop noncritical technical parameters for the completeness of the system evaluation or by regulatory guidance. Without inclusion in the contract, the contractor may not be held accountable for these parameters. Noncritical parameters may become critical as the system evolves.

Section III

System Evaluation Planning Process

5–11. System evaluation strategy overview

a. The system evaluation strategy defines the evaluation support to be provided to the systems acquisition process and identifies the necessary test, model, simulation, and analytic events needed to support the system evaluation process. To develop the system evaluation strategy, the system evaluator, in coordination with the T&E WIPT, must—

(1) Review requirements documents and the COIC.
(2) Address CTPs, AIs, and measures for evaluation.
(3) Identify the data requirements and data-generating events.
(4) Coordinate with the user and acquisition community.
(5) Provide the system evaluation requirements and objectives for the TEMP.
(6) Develop the SEP, to include test entrance criteria as appropriate.
(7) Provide system evaluation M&S requirements to the SSP.

b. All systems are developed to allow Soldiers, units, and commanders to conduct mission-level tasks and, thus, provide one or more operational capabilities. The system evaluation effort begins by defining what it means to be mission effective, suitable, and survivable for a specified unit receiving the system.

(1) Mission effectiveness pertains to the capability of the operational unit (that is, military units and Soldiers) to accomplish the critical mission tasks required to perform its assigned missions, as described in the MNS and ORD. Capability is the ability of typical operators and maintainers to accomplish needed critical mission tasks.

(2) Mission suitability pertains to the design characteristics (such as MANPRINT, RAM, integrated logistics, and tactical interoperability) needed to enable and sustain critical mission task accomplishment. Sustainability addresses the ability of the system to achieve and remain in an operable and committable state (that is, operational availability) during the course of conducting its missions.

(3) Mission survivability addresses the design characteristics needed to enable systems and operational units to avoid, evade, and withstand the effects of the threat in order to increase mission effectiveness.

c. As an extension to the system evaluation strategy, the SEP identifies important areas of study, prescribed measurements, and the data and informational needs of the system evaluation effort. These data gathering needs are identified in test plans over a variety of test events as discussed in chapter 6. The SEP shapes the relevant topics to be evaluated.

5–12. Development of the system evaluation strategy

a. The system evaluation strategy constructs a road map of the CE effort for the systems acquisition process (such as from concept to fielding). It focuses on both mission-level and system-level. The mission focus directly relates to the final determination of mission effectiveness, suitability, and survivability. The system evaluation strategy outlines the missions and mission tasks that will be studied and evaluated prior to LRIP, FRP, materiel release, and fielding. The complement to the mission-oriented portion of the system evaluation strategy is the system functional capability. System functional capabilities will be identified, studied, and assessed throughout the acquisition process. Linkage between the system functional capability developed by the PM and the supported mission task conducted by Soldiers must be clear. The system evaluation strategy outlines this mission-system linkage, and it is detailed in the SEP. The system evaluation strategy is developed in parallel with the acquisition strategy (see AR 70–1) and is developed as early in the systems acquisition process as possible. All aspects of performance, safety, and operational effectiveness, suitability, and survivability must be evaluated under realistic operational conditions. The iterative process of testing changes the emphasis of the system evaluations and assessments as the system evolves through design goals and moves towards IOT and the FRP DR. As appropriate, the system evaluation will reflect the system in a realistic environment with typical users, support, threat personnel, and equipment.

b. The TEMP (see chap 3) documents the T&E strategy, including the separate T&E cycles to be performed during the development and acquisition of the system. The system evaluation strategy is developed based on requirements identified in the ORD and the COIC (see chap 4), as well as other supporting documents (such as AoA, SSP, threat assessments, and mission area strategies under development). The overall T&E strategy considers combined or integrated testing and M&S to save resources and time and as cost-effective methods for overcoming limitations and constraints upon T&E. M&S may be used to achieve adequate test realism, support more economical, timely, and controlled test execution, and contribute to a more sufficiently comprehensive system evaluation.

c. The system evaluator develops the SEP in concert with development of the TEMP. The SEP is a system-level document that provides the integrated T&E strategy (such as the system evaluation strategy and the T/SES) to be used throughout the system's acquisition life cycle. While consistent with the TEMP, the SEP provides the additional detail to ensure the developmental, operational, and live-fire testing, including M&S and other events, are sufficient to satisfy the evaluation issues. If significant program changes occur, the SEP is updated or revised prior to milestone decision points.

d. The major questions to be answered become the evaluation issues. These issues include all the COI and supporting criteria and any AI developed to address areas covered by CTPs, KPPs, or other requirements. The system evaluator, in coordination with the testers, determines what data are required to answer the issues and identifies the supporting events as well as the conditions under which each event must be performed to ensure the data are adequate.

e. DoDI 5000.02 requires that all projects that undergo a MS A decision to have a T&E strategy. The Service component approved T&E strategy is to be submitted to OSD for approval. It primarily addresses M&S, identifying and managing the associated risk, and how to evaluate systems against mission requirements.

(1) There is no mandatory format for this early T&E strategy. Because pre-MS A systems will have neither an ORD nor COIs, the early T&E strategy will be based on the MNS. When an early T&E strategy is developed, it will become the basis for the T&E strategy in the TEMP.

(2) The early T&E strategy will follow the same approval process as the TEMP.

(3) The early evaluation strategy is jointly developed by OSD, ATEC, MATDEV, and CBTDEV.

5–13. Test and evaluation reviews

Reviews are conducted periodically to assess progress and readiness to proceed to the next step in the T&E process.

a. Early strategy review. An early strategy review (ESR) is held to review and approve the proposed system evaluation strategy that will be documented in the SEP. The approval authority is briefed on the overall methodology, including the supporting baseline correlation matrix (BCM), AIs, and the T&E input to the TEMP. The approved system evaluation strategy is the basis for developing the supporting T/SES. Concurrently, the testers and system evaluator are working within the T&E WIPT to provide draft input to the TEMP.

b. Concept in-process review. A concept in-process review is held to brief the approval authority on the development of the T/SES. Approval of the pattern of analysis (PA) and the data source matrix (DSM) is also obtained. The ESR and concept in-process review may be combined.

c. Test readiness review. TRRs are held to assess overall readiness of the system for test. For detailed information on TRRs, see chapter 6.

5–14. Threat considerations in system evaluation

a. Evaluation base. The system evaluation must be based on testing that accurately represents the threat projected to exist at post-IOC. The post-IOC year will be used as the basis to determine threat projection requirements. The TI member of the T&E WIPT will review threat support to testing as part of the Threat Coordinating Group process.

(1) System evaluation planning must reflect the threat against a supporting system or a system that is interoperating with the system under test (such as a computer system dependent on a separate communications system).

(2) If the threat (as described in the STAR) or if any of the threat systems cannot be fully addressed in testing, the limitations, as well as the testers' plan to compensate for the limitations, must be included in the TEMP. A test's threat limitations must be addressed in sufficient detail to provide an understanding of their impact on the test and thereby the impact on providing data and information with which to support the system evaluation.

(3) The SER will address the approved threat of the requirements document, as well as the threat projected to exist post-IOC as described in the STAR. The SER will separately address each element of the approved threat, as well as the approved threat in existence at the last milestone review, if different.

(4) As much as practical, actual threat systems will be used as targets or simulators during testing. When actual threat systems are not available, only validated and accredited threat simulators that have been accredited in accordance with this pamphlet will be authorized for use to support testing. Requirements for threat systems, simulators, and targets are to be coordinated with the Project Manager for Instrumentation, Targets, and Threat Simulators (PM ITTS).

(5) Transitioning threat intelligence assessments into instrumented field test arrays adequate to test a developmental system within the context of the COIC, exit criteria, and technical characteristics, is one of the more demanding challenges confronting testers and the system evaluator. Given resource constraints that preclude representation of a threat force with complete fidelity, testers and the system evaluator must be persistent and resourceful in seeking means to offset threat portrayal shortfalls to minimize their impacts as potential test limitations with emphasis on those aspects directly related to the COIC and AIs.

(6) Application of M&S techniques should be considered as a means to offset the impacts of a test's threat limitations and assess the impacts of uncertainties that exist in the test data.

(7) Smoke and obscurants and laser vulnerability will be addressed as a part of all threat considerations for electromagnetic and optical systems.

b. Threat Coordinating Group. The system-specific Threat Coordinating Group is an integrating body composed of the Army's CBTDEV and MATDEV organizations, T&E organizations, and the intelligence community to coordinate the provision of timely, consistent, and approved threat intelligence support throughout the acquisition cycle of a system. The TI establishes and chairs the Threat Coordinating Group as a subgroup of the T&E WIPT. For major and OSD T&E Oversight programs, the HQDA (DCS, G–2) Foreign Intelligence Director of Threat will establish the Threat Coordinating Group. For nonmajor programs, TRADOC or U.S. Army Materiel Command (AMC), in coordination with one another, have this responsibility. The system-specific Threat Coordinating Group performs the following functions:

(1) Assist CBTDEV and MATDEV to articulate their intelligence requirements and facilitate resolution of issues related to threat.

(2) Review and coordinate approval of STARs and threat TSPs and threat portions of system program management documents, such as the MNS, ORD, and TEMPs.

(3) Coordinate review of models, scenarios, and analysis for correct application and interpretation of threat.

(4) Review and coordinate threat support to testing with the Threat subgroup of the T&E WIPT to include scenarios and use of scenarios, simulators, surrogates, and targets.

(5) Identify threat and/or threat support issues and determine responsibility for resolution.

c. Threat Accreditation Working Group. After the initial threat coordinating group meeting, the threat accreditation working group (TAWG) should be convened. The TAWG is formed to accredit specific test application of threat simulators, targets, surrogates, and target arrays. See chapter 6 for details.

d. System threat assessment report. The Defense Acquisition Guidebook encourages a STA be conducted to support program initiation. The STAR (see AR 381–11) fulfills this requirement. It is the basic threat document supporting system development for all acquisition programs. It is used to define the threat environment in which a developmental system must function throughout its life cycle, typically at IOC plus 10 years. TRADOC develops and coordinates the STAR for systems for which program initiation occurs before MS B. For all other program initiation points, the STAR is developed by the MATDEV, who updates it annually.

(1) The STAR is written, approved, and updated continuously throughout the system development life cycle.

(2) The STAR is required for all ACATs; however, level of approval authority differs for oversight and non-major programs.

(3) The STAR includes the critical intelligence categories. The categories represent the threat capability or threshold established by the MATDEV, changes to which could critically impact the effectiveness and survivability of the system.

e. Threat in the test and evaluation master plan. Representations of threats used for T&E will be identified in the TEMP. Approval for their use, in accordance with AR 381–11, will be part of the TEMP coordination and approval process. The TEMP relates threat intelligence to test events, as depicted in the STAR/STA, in order to identify requirements for all categories of threat simulators/targets and simulations, and requires that threat system and simulator requirements be identified by type, number, and availability. Also required is a comparison with available projected threat systems or simulators and a statement that identifies major shortfalls. Target requirements are to be treated in a similar manner.

f. Issues and criteria. The COIC, defining acceptable standards of system performance, are formulated before the STAR. As a result, there may be differences between the threat outlined in the STAR and the threat considered in developing the CTPs and COIC/AI. This situation also can arise with the threat TSP, which may require modification to accommodate evolving COIC or exit criteria and test planning.

g. Use of threat simulators and targets. Whenever possible, actual threat systems are used during OT to represent an enemy force, but resource limitations usually result in the use of replicas, threat simulators, and surrogates, the functional characteristics of which approximate those of actual threat systems. Threat simulators generally are more costly and sophisticated than targets and are intended for reuse, and targets are devices that are designed to be engaged and destroyed.

h. Project Manager for Instrumentation, Targets, and Threat Simulators. The PM ITTS has the responsibility for the engineering, development, acquisition, fielding, life cycle management, and capability accounting of Army targets, threat simulators, and major range instrumentation for DT and OT. The PM ITTS is the executive agent for both the Army threat simulators and Army targets programs.

i. Threat simulator and target validation. Validation is the process used to determine whether a threat simulator or target provides a sufficiently realistic representation of a corresponding threat system to justify continuation of its development, use, or modification to restore or improve its capabilities to conform with current intelligence estimates.

(1) The PM ITTS determines when validation working groups (VWGs) are required, informs TEMA, and also participates in the meetings. TEMA determines whether a VWG will be chartered to manage the overall validation effort or that TEMA will chair a DA level VWG to conduct the validation effort.

(2) Validation is performed at key decision points during the life cycle of simulator or target: design specification review; IOC (acceptance); and operational (upon major modification) and periodically following acceptance for use in testing.

(3) The IOC report is approved by the Director, TEMA and is subsequently forwarded to DOT&E for final approval. After the MATDEV completes the design system review (DSR) report, the threat subgroup to the T&E WIPT will review the report and provide concurrence/non-concurrence comments to the developer. In turn, the developer is required to submit a one-page letter DSR report to TEMA briefly highlighting the results of the DSR report and addressing any unresolved non-concurrences. The operational validation report (VR) is completed by the system's developer/owner, which is submitted to TEMA for review and concurrence.

(4) PM ITTS chairs the DA VWG Planning Committee, which is the work group that does all of the extensive, real time planning for the DA VWG.

j. Organizational responsibilities. Because a number of organizations share responsibility for the complex and demanding task of integrating threat into T&E, AR 381–11 provides a detailed explanation of organizational responsibilities with respect to threat support. The process of integrating threat into T&E programs requires that DCS (G–3 and G–2), TEMA, AMC, TRADOC, ATEC, SMDC, and AMSAA coordinate closely and constantly throughout the acquisition process.

k. Required characteristics of threat support to test and evaluation.

(1) *Consistency.* The threat environments applied to testing of developmental systems must be derived from a baseline of DA-approved intelligence products. Threat portrayals for DT and OT of a system, although tailored for each test, must remain compatible throughout testing.

(2) *Continuity.* The planned portrayal of threat must be evaluated at each phase in the T&E cycle to ensure that related shortfalls are identified in T&E documents as test limitations and their impacts on the validity of the test are assessed. Efforts to incorporate the most current threat intelligence in test planning and to upgrade the fidelity of planned threat portrayals must be continuous.

(3) *Timeliness.* Intelligence estimates of the threat, even though they may treat specific aspects of future threat forces capabilities with uncertainty due to intelligence "gaps," must be provided to developers and testers on a timely basis to meet prescribed planning milestones throughout the T&E cycle.

(4) *Tailoring.* Threat must be tailored to each test to ensure that the simulated battlefield environment is adequate to test the developmental system in the context of the IOC threat it must counter. In defining the threat for developers, testers, and evaluators, implications of incomplete intelligence must be identified to them in terms of "gaps" and uncertainties to allow early consideration of the application of automated M&S techniques necessary to integrate relevant threat intelligence uncertainties into T&E processes.

(5) *Comprehensiveness.* The threat against the total system must be described and include supporting systems or other interoperating systems, such as a computer system dependent on a separate communications system. Threat surrogates need to be approved by DCS, G–2.

l. Lethality and survivability (see apps I and J).

(1) *Direct effect systems.* For those kinetic, chemical, and directed-energy weapons that have direct impacts against the threat force, effectiveness is measured in terms of lethality and survivability.

(2) *Indirect effects systems.* Other types of systems are designed to operate indirectly against threat systems by enhancing the lethality and/or survivability of a primary system, (for example, improving the mobility; command, control, and communications; or intelligence support of a lethal system). While the operational effectiveness of indirect systems cannot be measured by the direct impact they have on the threat force, they can be measured by the extent to which they either multiply the lethality, or increase the survivability, of a primary (direct effect) system.

(3) *Combined effects systems.* Some indirect systems and subsystems (such as communications and target acquisition), however, are subject to both lethal and non-lethal EW threats. Although testing may isolate and emphasize the EW threats against indirect systems, ultimately a determination must be made whether the indirect system measurably contributes to the operational effectiveness of either specific lethal systems or combat forces overall. These determinations are difficult and tenuous if indirect systems, such as intelligence systems, are evaluated against the threat of deception, or if EW systems are measured against enemy communications.

m. Threat modeling and simulation. Threat M&S should be considered as an adjunct to testing when developing the evaluation strategy. M&S can provide data when actual field testing is either infeasible or impractical due to factors of cost, test time length, unsuitability of maneuver space, terrain, weather, security considerations, safety, threat portrayal shortfalls, restriction on use of the electromagnetic spectrum, and limited instrumentation affecting other test resources. See chapter 6 for details on using threat M&S in testing.

5–15. System evaluation issues and criteria

The SEP defines the plan for the system evaluation and supporting events. It provides specific detail down to the MOE and MOP level. The system evaluator prepares the SEP in coordination with the T&E WIPT. Issues are the concerns expressed as questions that provide focus for the system evaluation. Criteria are the standards, or measures, that when achieved answer the issues.

a. The issues include both the COIC (see chap 4), developed by the CBTDEV, and the AIs, developed by the system evaluator. Issues for evaluation cover all aspects of a system applicable to the evaluation of operational effectiveness, suitability, and survivability.

b. The AIs complement and supplement the COIC and are derived from the ORD, CTPs, KPPs, and other performance parameters. AIs address the total system requirements rather than just the critical elements. The system evaluator develops the AIs in coordination with the testers, CBTDEV, and other members of the T&E WIPT. It is important to develop and comprehensively review the AIs because they must address all required areas not addressed by the COIC.

c. The elements of an AI set are the issue statement, scope, and measures (or set of measures) associated with the issue. The conditions for examining and standards for measuring a comprehensive issue are contained in the scope. Each element contributes to the cohesiveness of a complete evaluation issue. It is re-emphasized that answers to an issue may be provided by one or more means.

d. See chapter 4 and appendix E for the details on COIC format and content.

e. Categories of system evaluation issues.

(1) *Mission performance issues.* Mission performance issues are those that deal with determining how well the system does what it is designed to do. Such issues normally address the major functions of the system (for example, detecting, identifying, and engaging aircraft, or receiving, processing, and relaying message traffic). Mission performance issues generally address system level functions and do not address component functions.

(2) *Survivability and vulnerability issues.* Survivability and vulnerability issues are those that deal with a system's likelihood of avoiding being rendered ineffective by enemy action while performing its mission. DT typically

addresses the following factors: firepower (lethality), survivability (vulnerability), performance, safety, reliability, maintainability, durability, MANPRINT, ILS, and software. While OT measures may include the same areas as DT measures, they are from an operationally realistic environment and will normally include system signatures and exposure times, as appropriate. These measures determine ease of enemy engagement. See appendix I for a more detailed discussion of survivability and vulnerability.

(3) *Reliability, availability, and maintainability issues.* These three elements may be broken out separately or in terms of only reliability and maintainability when availability is not applicable. Reliability and maintainability will always address technical and operational aspects, whereas availability will only address operational aspects. See appendix K for definitions and a more detailed discussion of the RAM WIPT and the RAM scoring conference procedures.

(4) *Logistics supportability issues.* Logistics supportability issues deal with the impact of providing maintenance and operating support, as well as tactical automation support in both concepts and materiel. Maintenance support includes repair teams, procedures, the spare parts supply system, and materiel evacuation assets. Operating support must consider such expendable items as POL, air filters, rations, and ammunition. See appendix L for a more detailed discussion of ILS and logistics supportability.

(5) *Manpower and personnel integration and system safety issues.* See AR 602–2 and AR 385–10. Throughout the acquisition process, MANPRINT will be a factor in all T&E planning. MANPRINT addresses human performance considerations as they apply to a system. MANPRINT has seven areas of interest (that is, domains) that are considered in developing the evaluation issues: manpower, personnel, training, human factors engineering (HFE), system safety, health hazards, and Soldier survivability. MANPRINT issues examine management and technical efforts to ensure total system effectiveness by posing the question, "Can typical Soldiers, with the training given, perform these tasks to the standards under these conditions using this equipment?" See appendix M for a more detailed discussion of MANPRINT and appendix N for system safety.

(6) *Means of employment issues.* Means of employment consists of organization, doctrine, and tactics. Organization evaluation issues deal with how people are distributed by position and what equipment would optimize the system's effectiveness in the context of its operating environment. Such issues also examine the organization of the maintenance and other support units that must interact with the system's unit. Doctrine issues investigate the adequacy of planned doctrine for the employment of the system. These issues must consider doctrinal aspects of the unit or organization that hosts the system, as well as those aspects of supporting and supported units to optimize the effectiveness.

(7) *Interoperability issues.* Interoperability involves the technical ability to "talk to" other systems and the operational ability to exchange information/data that enhances mission accomplishment and force effectiveness. Interoperability issues examine the extent to which a system interacts with or does not interfere with other systems on the battlefield. The system is studied for its synergistic relationship in its operational environment. See appendix O for more details.

(8) *Transportability issues.* See AR 70–47. Transportability and deployability evaluation issues address the ability to move the system into a theater of operations and move it within the theater of operations consistent with the mission. These issues are sometimes considered as a separate, distinct element of operational suitability, rather than as a part of logistics supportability. Transportability issues may deal with airplane loading or internal and external helicopter loads. The examination must address not only the ability of aircraft to carry the load but also their availability (for example, numbers of carrier vehicles not otherwise committed). See appendix L for details.

(9) *Natural environmental testing issues.* Requirements documents include a statement of the areas or climatic conditions in which the system may be operated, stored, or transported. Systems under development are always tested in climatic chambers and usually undergo additional natural environmental tests to provide data on the synergistic effects of the climate. Type classification requirements include the completion of natural environmental testing in the basic climatic design type. Items designated specifically or primarily for use in extreme natural environments should successfully complete the extreme climatic tests for the specific areas of intended use. See appendix P for details.

(10) *Software issues.* Software considerations for battlefield automated systems, except for organization, doctrine, and transportability and deployability categories, must be made when forming the AIs. Although primarily found in mission performance functions, software extends to the remaining categories of system evaluation issues. Survivability and vulnerability issues, for example, may have a radar warning feature supported by software that warrants examination. Test, measurement, and diagnostic equipment (TMDE) is likely to be heavily software dependent. Each category should be examined to see if there is reason to include a software issue and criteria. Most software evaluations require some verification of the software's value and safety through testing. Software issues can involve IA. See appendix Q for a detailed discussion of software issues.

5–16. System evaluation tools

Evaluation planning is an iterative process that requires formal and informal analyses of demonstrated or potential system performance to meet the stated mission-level and system-level requirements against a specified threat and operational environment. Techniques that have been proven effective in evaluation planning include process analysis, design or engineering analysis, matrix analysis, and dendritic analysis.

a. Process analysis techniques. Process analysis techniques consist of thinking through how the system will be used in a variety of environments, threats, missions, and scenarios in order to understand the events, actions, situations, and results that are expected to occur. This technique aids in the identification and clarification of appropriate measures, test conditions, and data requirements.

b. Design or engineering analysis techniques. Design or engineering analysis techniques are used to examine all mechanical or functional operations that the system has been designed to perform. These techniques involve a systematic exploration of the system's hardware and software components, purpose, performance bounds, manpower and personnel considerations, known problem areas, and impact on other components. Exploration of the way a system operates compared to intended performance functions often identifies issues, measures, specific data, test events, and required instrumentation.

c. Matrix analysis techniques. Matrix analysis techniques are useful for analyzing any situation where two classifications must be cross-referenced. For example, a matrix of "types of data" versus "means of data collection" can reveal not only types of data having no planned means of collection but also redundant or backup collection systems. Matrix techniques are effective for tracing a system's operational requirements through contractual specification documents, as well as issues and criteria, to sources of individual data or specific test events.

d. Dendritic analysis techniques. Dendritic analysis techniques are an effective way of reviewing COI to determine the point where actual data requirements, test measurements, and modeling assumptions and predictions can be identified. Issues are successively broken down into sub-issues, measures, and data requirements in a root-like structure. In this approach, the objectives are used to clearly express the broad aspects of evaluation related to the COI and the overall purpose of the data. Measures are developed as subsets of the objectives and are designed to treat specific and addressable parts of the objectives.

5–17. Data sources for system evaluation

The continuous system evaluation strategy is developed to assess all aspects of a system's technical parameters and operational performance. Therefore, the system evaluator uses all credible sources of data to provide information relative to technical performance, qualification of components, compatibility, interoperability, survivability, vulnerability, lethality, transportability, RAM, manpower and personnel, safety, ILS, correction of deficiencies, accuracy of environmental documentation, and refinement of requirements. The system evaluation also provides information relative to doctrine, tactics, and training.

a. Developmental testing and operational testing. See chapter 6.

b. Foreign comparative testing. The objective of the FCT program is to reduce duplication in research and development and provide cost and performance advantages. See AR 73–1.

c. Models and simulations (see para 5–21). The system evaluator determines availability of and the need for M&S analyses during development of the SEP.

d. Market investigation. The data collected during market investigation provide information on the ability of items to fill operational requirements.

e. Other military services, other U.S. agencies, foreign governments, and data collected by private industry. Use of existing data is highly encouraged to support the system evaluation. In the case of foreign governments, agreements may be in place or needed to support the exchange of such data.

f. Warfighting experiments. Warfighting experiments may consist of AWE or CEP that are conducted by battle labs, Army proponents, and Joint Forces Command to provide data in support of the requirements determination, the force development, and the technology transition processes. (See AR 73–1.)

g. Force development test or experimentation. The FDT/E program examines the effectiveness of existing or proposed concepts or products of doctrine, training, leader developments, organization, and Soldier development. (See AR 73–1.)

h. Advanced concept technology demonstration and advanced technology demonstration. These demonstrations provide pre-acquisition data in support of warfighting concepts and should result in a more comprehensive requirements document. The system evaluator uses the data generated during these demonstrations if the technology being demonstrated results in an acquisition program. (See AR 73–1.)

5–18. Baseline correlation matrix

The BCM is a tool used to analytically structure all evaluation requirements for identification and documentation. The BCM presents a crosswalk of the requirements from all the applicable requirements documents and COI. The crosswalk provides the capability to analyze and compare requirements and assists in the identification and definition of AIs and measures. The BCM is used to ensure that the system requirements documents are consistent and to flag those cases where inconsistencies exist.

a. Spreadsheet format. The BCM spreadsheet format (see an example at table 5–1) shows requirements in the left column with source documents organized across the remaining columns. The resulting cells record the stated information as documented in the specific source document. This process provides for easy assessment of consistency of requirements and identifies areas that are not addressed but that are required for a comprehensive evaluation as AIs. Technical and operational requirements are indexed to the evaluation issues in the left-most column and are traced through the requirement development process to the measures in the right-most column that will be gathered in testing. The measures are used to ensure the data collected are comprehensive enough to address all the different ways in which a requirement may have been stated. Entries should include the paragraph number from the source document and a summary of the capability, measure, and threshold when applicable. The BCM should include, but not be limited to, the following column headings if the applicable documents exist:

(1) System requirements categories.
(2) Mission need statement (MNS).
(3) Operational requirements document (ORD).
(4) Latest AoA. Correlate the MOE with system issues and requirements if possible. Resolve inconsistencies.
(5) System specification or RFP if the document details operational requirements. For NDI, the RFP and system specifications may be the primary requirements documents available.
(6) Critical technical parameters (CTPs).
(7) Critical operational issues (COIs).
(8) Additional issues (AIs).
(9) System training plan (STRAP).
(10) System safety management plan (SSMP).
(11) System manpower and personnel integration management plan (SMMP).
(12) Computer resource management plan (CRMP).
(13) Measures. The measures give an indication if the system requirements can be evaluated. If satisfactory measures cannot be defined, the system evaluator cannot evaluate the system requirement as stated.

Table 5–1
Sample baseline correlation matrix

System requirement	MNS	ORD	System specification	COIC	AI	SMMP	CRMP	MOE/MOP
1.0 Firepower	CAL must provide a high degree of protection from enemy aircraft raids.	2.3 CAL probability of kill=0.96 per enemy plane when raid size is < 20 planes.	1.2 CAL probability of kill=0.96 per enemy plane when raid size is < 20 planes.	1. Issue. Does the CAL provide an improved capability of kill enemy planes? 1.1 Criteria. CAL will have a probability of kill < when raid size is < 20 planes.	5. Issue. Does the CAL retain capability of kill in an EW environment? (No criteria)			1.1.1 Pk=#K/T#Tgts. #K=# enemy planes killed in given battle sequence T#Tgts=total # targets in given sequence. 5.1 Pk=(etc.) 5.2 Pk=(etc.)
		2.7 CAL must have a firing rate of 1 round per	1.3 CAL must have a firing rate of 1 round per	2. Issue. Does the CAL have an effective firing rate				2.1.1 MTT Launcher Firing Rate=(Sum of DUREI)/(Sum of #U).

Table 5–1
Sample baseline correlation matrix—Continued

		launcher every 5 seconds.	launcher every 3 seconds.	during a typical battle scenario? 2.1 Criteria. CAL's firing rate of 1 round per launcher/5 sec.				DUREI=duration of engagement i. U=# launcher for launcher 1 in eng
2.0 Target Location	4.2 CAL must detect, identify, and engage targets with a high probability at a distance before threat aircraft can deliver ornance.	3.1 CAL must detect target with probability 0.91 at a distance of < 2 miles.	2.5 CAL must detect target with probability 0.91 at a distance of < 2 miles.	3. Issue. Does the CAL accurately detect enemy targets in an operational environment? 3.1 Criteria. CAL will detect enemy target with probability < 0.91 when target is < 2 mi.				3. Issue. Does the CAL accurately detect enemy targets in an operational environment? 3.1 Criteria. CAL will detect enemy target with probability < 0.91 when target is < 2 mi.
		3.2 CAL operator must correctly identify target with 0.98 probability.	5.7.1 The CAL weapons sight will have a resolution of 0.3 milliradians.	4. Issue. Does CAL correctly identify targets in the field? 4.1 Criteria. CAL will correctly identify 98% of the targets it detects. 4.2 Criteria. (etc.)				4.1.1 Pi=#I/#D. #1 is #enemy planes correctly ID in a given battle sequence. #D is # enemy planes detected in a given battle sequence.

b. Development of the BCM is an evolutionary process. As requirements from each new baseline document are added, they are compared to the requirements already established in the BCM. By tracing the consistency of the requirements for wording, measures, units, and specific values, discrepancies are found at a time when their impact can easily be minimized. If an inconsistency, omission, or other change that is not directly traceable to an earlier requirement is noted, it must be justified or rectified. The issues for evaluation (such as CTPs, COI, and AI) are examined to ensure that each is covered by an adequate set of measures. The end product is a consistent, fully justified set of operational measures that is a firm foundation for the system evaluation. The BCM is included as an appendix to the SEP. See paragraph 5–15 for a complete discussion of issues in a system evaluation.

c. Streamlining of the BCM is permitted for nonmajor programs. The system evaluator may consider combining the DSM and the BCM, if appropriate and with the agreement of the T&E WIPT.

5–19. Data source matrix

The DSM identifies all supporting test and simulation events and allocates MOEs/MOPs to those events. The purpose is to provide a crosswalk of all measures to the identified data sources. The matrix is structured to show each issue, criteria, and supporting measure in the left three columns of the spreadsheet and each identified data source across the

remaining columns. Measures are allocated to the most appropriate event for generation and collection of data. Each measure must have at least one primary data source. The DSM shows the contributions of each data source to the measures, enabling event planners to properly scope the requirements of the events. The DSM assists in identification of unnecessary testing. The DSM is coordinated with the T&E WIPT. A sample DSM is at table 5–2.

Table 5–2
Sample data source matrix

Issue	Criteria	MOE/MOP	IOT	FDT/E	DT	Kr test	M&S	Market survey
1. Capability of kill improved?	1–1. Pk if < 20 planes	1–1–1. Pk=#K/T#Tgts 1–1–2 (etc.) 1–1–3 (etc.)	P		P	S	S	P
2. Firing rate effect?	2–1. 1 round per launcher every 5 sec	2–2–1 R=S =; DUREI/S #U 2–2–2 (etc.)		P	P			
3. Detect accurately in operational environment?	3–1. Detect 91% @ 2 miles	3–3–1. Pd=#D/T#Tgts 3–3–2. (etc.)	P			P		S
4. Identify targets?	4–1. Identify 98% of detects	4–4–1. Pi=#I/#D	P					
5. (etc.)	5–1. (etc.)	5–5–2. (etc.)	P	P				

Notes:
P = primary data source; S = secondary data source; Kr = contractor.

5–20. Pattern of analysis

The PA is a major element in OT event planning. It provides the transition between the measures contained in the approved SEP to the identification of the actual data elements required to calculate a response for the measures. The PA is required for all operational test events and becomes an appendix to the EDP for the event. It is staffed, approved, and distributed as part of the overall requirements for the EDP. The PA is normally prepared in dendritic format and depicts, in hierarchical format, the relationship of COI and AI along with the associated criteria into measures and related specific test and/or evaluation questions, data requirements (additional related questions), and/or data elements. The PA can be displayed in narrative terms or graphically and is normally developed by the tester in conjunction with the system evaluator.

a. The initial portion of the PA is developed by the system evaluator as a function of the development of the detailed evaluation requirements following approval of the system evaluation strategy. Using the approved strategy and the COI and AI, the system evaluator develops the initial dendritic portion of the PA to organize requirements under the broad areas of effectiveness, suitability, and survivability. Each issue or requirement for the issues is assigned to one of the functions of effectiveness, suitability, and survivability, as appropriate. Measures are developed to address requirements to answer each issue (without concern as to the data source). This process may suggest that a draft AI could be better incorporated in another area and eliminated as a separate issue. The testers and system evaluator use these measures to support development of the required data sources and the DSM. The tester finalizes the PA and develops the individual data elements by using the measures assigned to a specific event.

b. As part of the process, the testers and system evaluator establish a priority for each measure using the priority levels 1, 2, 3, or 4. A priority assists if test resources are subsequently changed necessitating a change in the test design—

(1) *Priority 1.* Measures required for answering the COI for effectiveness, suitability, and survivability. Measures that are directed for inclusion by others who approve OR disapprove test plans (for example, DUSA (OR) and DOT&E).

(2) *Priority 2.* Supportive measures that mitigate the level of risk in answering issues, check-out areas resulting from CE lessons learned, as well as critical mission essential software functions that did not work well during DT.

(3) *Priority 3.* Measures that are prudent to collect that support the issues (for example, causality or diagnostic).

(4) *Priority 4.* Measures that are recommended for inclusion by others in the T&E community (for example, AMSAA, PM, or U.S. Army Training and Doctrine Command system manager (TSM)).

c. The ultimate goal of the PA is to link COI and AI with simple, measurable data elements. The key to establishing this link, within the process of subdivision, is the identification of each MOE or MOP. MOEs focus on mission accomplishment and mission utility. They serve as the higher level measures. MOPs normally can be expressed numerically in observable terms, which represent identified dependent variables by which the system performance can be characterized. Data elements are the lowest level of information collected and generally require recording of an item of information that is factual, based upon observation or instrumentation, and requires no linkage with any other data element to record. A quality PA is used by the tester to assist in the planning and development of requirements for the event scenario or other scheduling plan and the data collection and management plan. See paragraph 6–43*g* for further details on the PA.

5–21. Modeling and simulation

a. M&S is always considered to support the evaluation of systems as they proceed through the life cycle. Use of M&S includes, but is not limited to—

(1) Identification of test parameters and key measures.

(2) Determination of high risk areas.

(3) Prediction of system performance.

(4) Assisting in the allocation of resources.

(5) Stimulation or stressing of the system under test for operational realism.

(6) Assessment of system capabilities in situations that cannot be tested.

b. System models in evaluation. System models that are used in system evaluation should be the same as, or traceable to, the models used for concept development, AoA, system design, and production. Synthetic test environments may also be reused for training, operations planning and rehearsal, and subsequent concept developments. Participation by the system evaluator on the ICT/IPT, as part of the system collaborative environment, will allow the system evaluator to know what M&S are required, and provide input and recommendations for existing M&S already used by the testing community. Additionally, the evaluator may also see an opportunity to accredit existing M&S for system evaluation purposes.

c. Use of modeling and simulation. M&S can be used extensively to support the CE process that includes the software development process. Testing of complex systems can be large in scope and require conditions that are difficult, if not impossible, to create short of actual combat. The practicalities of cost, time, test range space, availability of advanced threat systems/surrogates, and safety, will necessarily limit test planning and test data availability. M&S can address these limitations. System evaluation may require physics-based M&S to extend the understanding of the available test data and to extrapolate or interpolate to conditions that cannot be tested due to constraints and limitations in the test environment. While M&S does not replace testing, it is a complementary tool in the CE process.

d. Simulation, test, and evaluation process. USD (AT&L) policy requires that simulation, test, and evaluation process (STEP) be an integral part of the TEMP. The STEP Guidelines describe how T&E can be enhanced with the application of M&S tools. Testing produces M&S with increased credibility and allows for the assessment of system performance in areas and under conditions that might not be otherwise available with conventional testing methods. Simulation support planning must consider how M&S will be used in T&E and, in particular, VV&A requirements. The SSP should be cross-walked to the TEMP at each TEMP update to ensure STEP objectives can be met. The underlying approach to testing will be to model first, simulate, then test, and then iterate the test results back into the model. Figure 5–2 depicts typical uses of M&S in pre-test, test, and post-test applications, to support STEP methodology. The model-test-model process begins with the selection of the appropriate M&S tools to support the test design. Special emphasis is put on predictive analysis to ensure the development of meaningful, cost effective tests. The following paragraphs discuss the three phases of the model-test-model methodology:

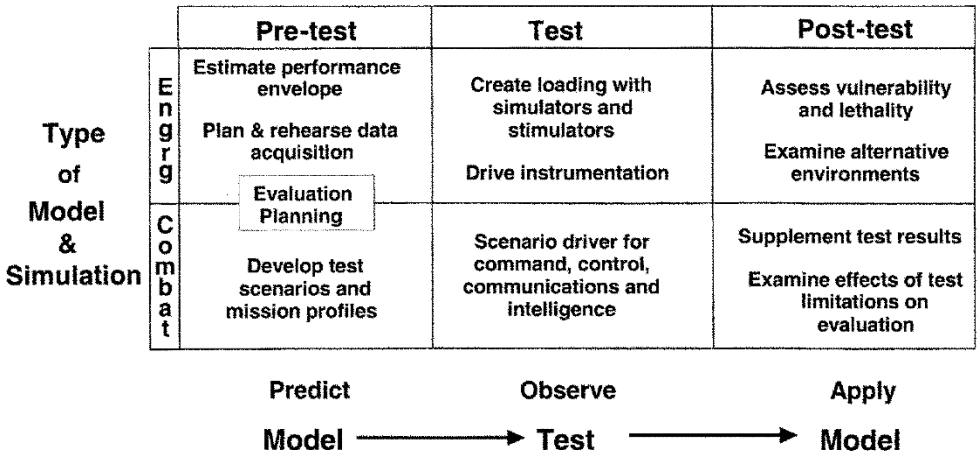


Figure 5–2. Models and simulation applications

(1) *Pretest modeling phase.* Pretest modeling estimates a range of test results prior to conduct of record trials/events. These results may aid the tester in supporting test design and test scenario development. Normally the pretest phase addresses the adequacy of test profiles/scenarios to support the test objectives. For example, does the planned test scenario provide the opportunity to collect information at the required ranges of engagement or ranges of communications for the system evaluation? Additionally, pretest M&S can be used to make more efficient use of test resources to avoid impractical use of test assets. If M&S shows that certain levels of countermeasures are expected to render the test item ineffective, sufficient testing to define the envelope of these levels must be conducted to validate the M&S predictions. M&S can be used to scale resources such as targets, warheads, or countermeasures in order to obtain equivalent MOE given constraints of resources, ranges, and test units. M&S can also be used to train test personnel, support test design (for example, number of trials, size of Blue and Red forces, check execution timing, plan location of test support equipment, validate threat surrogates/simulators), estimate key factors/conditions that most impact system performance, and develop and refine test design matrices.

(2) *Comparison of modeling and simulation with test results phase.* Comparison of M&S and test results begins with conduct of the test. Extensive work is required to develop adequate operational realizations of systems in combat models. The model results and test results must be compared to determine the significance of differences that may occur. The comparison must assess if calibration of the model is appropriate. Calibration should be conducted when it is determined that model components must be adjusted before any further application of the model will be accredited. Examples of model components critical to accreditation for T&E purposes include weapon system algorithms, man-machine and environmental interfaces, and the model scenario representation.

(3) *Post-test modeling phase.* The final phase of the process is the use of the model to make additional estimates. These estimates may supplement test results. Issues for evaluation and the completeness of the test will determine exactly what modeling will be required. Listed below are examples of how M&S may be used to supplement and extend test results as well as explain unexpected test results:

(a) Applying MOEs/MOPs to situations other than those tested (running many iterations based on trial results, varying terrain, varying force sizes).

(b) Investigating potential benefits of product improvement or changes in doctrine or organization.

(c) Analyzing the sensitivity of the evaluation findings to known limitations in approximating realistic MPs, for example, types of countermeasures that could not be played.

e. Army modeling and simulation guidelines. The Army's "Guidelines: Use of Modeling and Simulation (M&S) to Support Test and Evaluation (T&E)" provides detailed information on the application of M&S to T&E, verification and validation (V&V) of M&S, as well as planning for and sources of M&S. It also provides points of contact, examples of M&S use in weapon system development, and integrated VV&A of M&S in the life cycle management process. It is available at the website for TEMA. The use of M&S in conjunction with T&E should be documented in the system's TEMP and SSP. The SSP provides a summary of the T&E approach and appropriate test resources cross-referenced to the TEMP. The TEMP and the SSP ensure that M&S and test resources are allocated throughout all phases of the acquisition cycle.

f. Modeling and simulation in system evaluation. During development of the system evaluation strategy, the system evaluator, in coordination with the testers, determines the M&S requirements during development of the initial T&E strategy, including determining if appropriate M&S exists or if it must be developed. A consistent and traceable set of tools should be used throughout the T&E process to ensure consistency and validity of evaluation results. The model-test-model methodology supports pre-test analysis, test execution, and post-test analysis.

g. Modeling and simulation use during pre-test. Mission-level simulation is used during pre-test analysis to design the test scenarios, determine test conditions, and plan the sequence of trials. Timing of events can be planned, control variables examined, and test objectives evaluated in force-on-force or command and control environments. Using the system model or distributed product description, the tester and/or system evaluator can simulate the test mission to time events, examine control variables, and select the best places to place instrumentation or collect data.

h. Linkage of models. The force-on-force combat or war-gaming models that assist in the evaluation of the system's synergistic contributions to total force effectiveness may already have been used in generating the ORD or conducting the AoA. Use of the same models to design and drive operational test scenarios promotes linkage of test design to test requirements (such as TEMP, SEP, ORD, and MOP/MOE). They are primarily applied to address force-on-force issues for battalion and larger force structures, and can provide affordable realism without very large deployments. Throughout test execution, physics-based, or empirical models of expected system performance, can be used to control the test instrumentation, and validate the data in real time, during the execution of live tests of complex systems in complex environments. The same or similar models can be used to investigate excursions of system performance under conditions that are not tested. High performance simulators and stimulators generate and render synthetic environments and stimuli to induce, in the system under test, the same response that the actual environment or stimuli would in a battlefield situation.

i. Modeling and simulation use during post-test. During post-test analysis, M&S applications support system evaluations by expanding the test envelope and extrapolating system performance conditions to realistic environments or non-testable conditions. As M&S applications are validated, calibration data are fed back into the pre-test models. Thus, the simulation may be validated by the actual live test exercise results, and the test exercise may gain credibility from the comparison with the simulation.

j. Modeling and simulation considerations in live test. The selection of M&S tools should be coupled with concurrent considerations for selection of live test events to ensure the approach developed to execute the evaluation strategy is the most cost effective. Inherent in this process is the need to validate data sources. Live tests must be verified for efficient and effective design and validated to ensure that environmental conditions are appropriate and sufficient and that specific issues (information voids) are adequately addressed. M&S must be verified for logical stepwise process and use of sound software engineering techniques; validated for output, relative to input, that is comparable to real world observations; and officially accepted (accredited) as a source of credible data for a specific application.

k. Verification, validation, and accreditation. See DA Pam 5–11. A basic M&S tenet is that the use of any M&S in support of, or supplementation to, T&E is that the M&S be accredited if its results are used in the system evaluation. The Army requires VV&A of Army M&S as early as possible in the developmental process. The VV&A methodology must be tailored to the specific characteristics of the system being acquired.

(1) Verification is the process of determining if M&S accurately represents the developer's conceptual description and specifications and meets the needs stated in the requirements document. The verification process establishes if the simulation correctly performs the intended functions and the extent to which the simulation has been developed using sound systems engineering practices.

(2) Validation is the process of determining the extent to which M&S accurately represents the real world from the perspective of the intended use of the model or simulation. Validation has to do with the fidelity of M&S, which is judged by several factors, one of which is its ability to predict the known or best estimate of the behavior of the real system when subjected to the same stimuli.

(3) Accreditation is an official determination that M&S is acceptable for its intended purposes. It is based on experience and expert judgment and includes consideration of the extent to which V&V has been accomplished.

(4) Table 5–3 shows VV&A documents and responsibilities.

Table 5–3
Verification, validation, and accreditation responsibilities

VV&A	M&S sponsor	M&S developer	Accreditation action officer
V&V plan	Responsible	Assists	Use/assist
Verification	Responsible	Performs	Aware/assist

Table 5–3
Verification, validation, and accreditation responsibilities—Continued

Validation	Responsible	Assists	Aware/assist
V&V documentation	Responsible	Assists	Awareness
Accreditation plan[1]	Assists	Assists	Responsible
Accreditation request[1]	Assists	Assists	Responsible
Accreditation report	Assists	Assists	Responsible

Notes:
[1] The signature authority for accreditation plans and accreditation requests is the approver of the document in which M&S is used.

5–22. Development of measures of effectiveness, measures of performance, and data requirements

a. Definition for measure of effectiveness, measure of performance, and data requirements.

(1) MOEs are quantifiable elements of operational effectiveness used in comparing systems or concepts or estimating the contribution of a system or concept to the effectiveness of a military force. They express the extent to which a system accomplishes or supports a military mission.

(2) MOPs are quantifiable units of measure (such as miles per hour) that describe the manner in which a given function or task should be accomplished.

(3) A data requirement is a quantitative or qualitative piece of information that is relevant to the determination or categorization of one or more MOP. Data requirements can consist of measures (such as velocity, range, elapsed time, calculated distance between two points, or number of rounds fired) that are determined from data elements. Data elements are the lowest level of information collected and only require direct observation, timing, or recording by one person (or piece of instrumentation) at a single location at a single time. Example of data elements are start and stop times, position location, round fired, type target, light level, and mission-oriented protection posture (MOPP) level. A data requirement does not generally involve summary statistics (such as mean, median, or percent). Associated data requirements and resultant test factors and conditions are specified in the SEP, as appropriate. The system evaluator identifies data needed to support the planned evaluation and indicates those that are required from testing. The test designer includes these data requirements and derives additional data requirements needed for test control, diagnosis of problems, interpretation of the data, and quality assurance (such as the tester typically adds the data requirements necessary to track system utilization in accordance with the OMS/MP).

(4) A COIC criterion consists of a measure (that is, either a MOE or MOP) with a quantitative threshold value. A criterion may vary in complexity depending upon the system.

b. Evaluation planning objectives. Each planning method leads to more substantive information that aids in understanding the system response. The system evaluator plans for not only the estimation of system capability but for an understanding of why the capability is as it is and for estimating how that capability might be expected to change as the system matures. These methods also help in the early identification of required instrumentation and data organization.

c. Decomposition of issues and criteria. The system evaluator uses a dendritic process for developing logic trees and work breakdown structures (WBSs) for breaking down issues and criteria into MOEs/MOPs. Factors and conditions are integrated and necessary event dendritics are developed to define the data requirements. A MOE quantifies the extent to which a system attains the criterion. The MOE (that is, a higher level measure that is mission-oriented) generally encompasses one or more MOPs. For example, in a communications network, a MOE would be the degree to which the system supports division command and control. The MOP might be completion rate or availability of radiofrequency (RF) links. In an example of an air defense system, the MOE may be the degree to which the system protects against hostile air attack. The MOP might be the ability to detect or engage.

(1) The issues define the relevant questions that must be answered in the system evaluation. COIC criterion statements typically identify the primary MOE. The system evaluator expands and clarifies the primary MOE into a functional dendritic that covers supporting MOPs and data requirements and data elements appropriate to the analysis of the issue. As a vehicle for discussing the development of MOPs and data requirements, an example issue, associated scope and criterion is presented in figure 5–3. The example presents a typical issue and criterion and is used to illustrate the process used to develop appropriate MOPs and data requirements. The criterion presents two obvious MOPs, and the scope presents considerations relevant to factors and conditions that need to be addressed when answering the issue.

Issue. Is the *** system effective at determining prioritized target information to support *** in the close support role?

Scope. This issue addresses the speed and accuracy with which the *** system can search, detect, and locate heat emitting targets in the European Theater. The probability of detecting a target will be examined based upon the type of target, its IR cross-section, *** system speed, search pattern, and target density.

Criterion. The *** system must have a 90% chance of detecting threat vehicular targets within two minutes and locating them within a 25 meter CEP accuracy.

Rationale. State reasons why the above are required for the evaluation.

*** represents the name of the system

Figure 5–3. Sample issue and criteria set

(2) Close examination of the issue in figure 5–3 shows many questions not explicitly stated that need to be answered to understand the ability of the system to locate targets:

(a) What constitutes a target?

(b) How will false targets be handled?

(c) What constitutes a target presentation?

(d) What constitutes a correct detection?

d. Evaluation planning questions. After answering these questions and defining the terms, additional questions become relevant. Accordingly, the planning methods help identify types of questions that lead to a more thorough and well structured database in support of the system evaluation:

(1) Are any of the functions accomplished by the system causing deficiencies in the time or accuracy of location?

(2) Are there factors or conditions that lead to deficiencies in time or accuracy of location?

(3) Are there areas in which training or man-machine interface could be modified to improve target location?

(4) Are there learning or other trends associated with target location measures?

e. Developing the data requirements. After the system evaluator identifies the primary functions of the system and these functions are broken out into secondary (and sometimes tertiary) functions and into MOPs, the MOPs are divided into the set of data requirements. For the example shown in figure 5–3, the primary mission of providing prioritized target information is quantified in the criterion statement. The functions that support successful execution of the primary mission include searching the target area, detecting targets in the area searched, identifying and classifying as red or blue the targets detected, prioritizing the identified targets, locating the prioritized targets, and tracking the moving targets which have been located.

(1) To search a target area effectively, the system needs to cover the search area and do it efficiently. Dendritic development encourages the following type of questions, the answers to which strengthen the evaluation planning:

(a) How does one measure coverage and efficiency?

(b) How do inadequacies in searching the target area affect the MOPs?

(c) What is special about the system that is relevant to searching and that can be quantified?

(d) What makes a good detection?

(e) What are the capabilities of the system that impact or aid detection?

(f) How does discrimination between true and false targets impact detecting true targets?

(g) How does the success of the search function impact the detection success?

(h) How is classification success determined and how is it impacted by validity of the target?

(i) Is efficiency a consideration?

(j) What is correct prioritization? How is it measured?

(k) How do undetected targets affect prioritization success?

(2) The dendritic breaks the primary mission (for example, providing prioritized target information) into lower level functions supporting MOPs and then into data requirements. Each end point consists of measurable data that are traceable to the issue through the dendritic. This approach gives a reviewer an organized way of seeing how the data requirements were derived, and promotes understanding of the relationships between measures and data requirements.

(3) MOPs may be impacted by test variables, scenarios, and conditions. These factors represent independent variables used to characterize test events and are used to categorize, analyze, and evaluate outcomes of test events.

(4) Based, in part, on the analysis concept, the system evaluator determines the appropriate factors and conditions, together with the associated degree of control, and presents them in the form of a tabular list. The tabular list typically requires footnotes with accompanying discussions to clarify how the proposed types of control measures will ensure that appropriate numbers of valid events occur under various combinations of test conditions. Table 5–4 provides a typical listing of factors, types of control, and conditions for a typical scenario.

(5) The process continues with the development of the event dendritics. Like the functional dendritic, the event dendritic consists of a hierarchical decomposition of system functions into data required for analysis and evaluation. However, instead of dividing these functions by MOP relevant to specific issues and criteria, an event dendritic decomposes these functions by the sequence of events performed. (See chap 6.)

f. Data requirements planning. The end product of the functional dendritic, the factors and conditions chart, and the event dendritic, is the set of data needed for a comprehensive system evaluation. Each of the three approaches may need expansion based on the results of the other two. Their completion is an iterative process, and the products produced form the foundation for the system evaluation. The perspectives of each approach differ and determine a complementary, albeit different, set of data requirements. Without question, these examples can be expanded to include data requirements, MOPs, and factors not shown. The examples show the thought process and the products that lead to a comprehensive set of data requirements and an associated database that supports a comprehensive system evaluation. The functional dendritic and the factors and conditions contribute to the analysis planning. The factors and conditions chart forms the foundation for experimental design development, and the event dendritic forms a natural organization for the data.

Table 5–4
List of typical factors and conditions

Factors	Control	Conditions
Range of engagement	Systematically varied	100–500, 501–900, 901–1, 300 meters
Light conditions	Systematically varied	Day, night
Target movement	Systematically varied	Moving, stationary
Threat arrays	Systematically varied	IAW threat support package
NBC	Systematically varied	No MOPP, MOPP II, MOPP IV
Terrain (Phase I)	Systematically varied	Flat, rolling
Terrain (Phase II)	Tactically varied	Rugged, swamp
Enemy action	Systematically varied	Attack, defend
Battlefield obscuration	Systematically varied	No smoke, smoke
EW environment	Systematically varied	IAW threat support package
Personnel	Held constant	5th-95th percentile
Organization	Held constant	Battery level
Doctrine/tactics	Held constant	IAW D&O support package or IAW TRADOC support package
Logistics support	Held constant	ORG, DS
Communications status	Tactically varied	Radio-voice, radio-digital
Enemy target	Tactically varied	Troops, vehicle, bunker
Weather	Uncontrolled	Rain, dry, snow
System operating status	Uncontrolled	Fully operational, degraded mobility, degraded firepower, non-operational

g. System evaluation plan coordination. The system evaluator will coordinate the SEP with the CBTDEV or FP and PM or MATDEV on a regular basis during development so as to seek confirmation of understanding of the system (materiel and operational), its employment and sustainment, and evaluation measures and support for the planned system evaluation. Such coordination should be a continuation of the ICT effort that began with development of the ORD and COIC. As TEMP preparation gets underway with the T&E WIPT, the system evaluator coordinates the SEP with the full T&E WIPT.

Section IV

System Evaluation Conduct

5–23. Development of the event design plan

Based upon the DSM in the approved SEP, the event design requirements for each data source are developed. Event design requirements ensure that the essential data requirements needed for the system evaluation are obtained. An EDP is prepared for each OT and, when required, for DT. The EDP contains details on the overall test design, methodology, data management, and other requirements for the test or event and ensures that the essential data requirements needed to support the system evaluation are obtained.

5–24. Analysis and evaluation of measures of effectiveness and measures of performance

a. Issue resolution. The system evaluator develops the logical process that is intended for use in resolving the issue. This includes deciding how the data from the identified sources will be integrated and how anticipated constraints on the realism or the completeness of the data will be treated. The system evaluator develops the steps used to interpret analyses; how and where modeling, simulation, or military judgment will be used; and when appropriate, how conclusions on individual criterion will be integrated to resolve the issue. The system evaluator determines the comparisons that are anticipated and the estimates that will be made and ascertains their utility to the system evaluation.

b. System evaluation strategies. More than one strategy can be used to address different aspects of an issue, and occasionally, it may be appropriate to use more than one strategy to address the same aspect. Discussion of each aspect of an issue is to include factors, conditions, and operational scenarios appropriate to the system evaluator's plan to investigate discrimination between the systems, organizations, methods of operation, or procedures. Three basic comparative evaluation strategies are typically used—

(1) Comparison of new or competing system capability to the corresponding capability in the system being replaced (for example, baseline).

(2) Comparison of new or competing system to a predetermined standard.

(3) Comparison of an organization's capability with and without the new system.

c. Analysis approach and concept.

(1) An analysis approach is the framework within which data for all MOPs will be analyzed. The system evaluator identifies analytical steps planned to explore and understand the data, integrates data from appropriate sources, summarizes or re-express the data, estimates parameters, and determines trends or otherwise explores the data in a manner relevant to the evaluation of the data set.

(2) The analysis concept is the anticipated framework within which data for the issue will be analyzed. The system evaluator identifies how judgmental criteria and weights will be applied and identifies anticipated graphical or arithmetical techniques and the degree to which the analysis will be exploratory (that is, finding out what the data are trying to say) or confirming (that is, using formal statistical inference to answer predetermined questions).

(a) A good analysis concept serves as a road map for the analyses that are intended to identify or support evaluative conclusions. It is not meant to be rigidly followed if the actual data or other circumstances lead to a more appropriate procedure. The use of decision support system tools is an aid in developing the analysis concept.

(b) The system evaluator identifies the specific techniques appropriate for making the comparisons or estimates called for in the analysis concept. For each comparison or estimate, the chosen technique must be planned in sufficient detail to establish a sound analytic treatment for the operational question being asked. Alternative techniques are sometimes appropriate, but no attempt should be made to perform each and every alternative form of analysis.

d. Data assumptions. After the test, actual data often render even the best-planned techniques irrelevant or inappropriate. The system evaluator should identify the assumptions associated with the data, the distributions, and the use of proposed analysis techniques. The extent to which the results from the assumptions are likely to be sensitive to

deviations, especially as they impact calculations of planned confidence intervals and significance statements, should be addressed in planning.

e. Data independence. The independence of data points must be preserved. The many factors that typically influence the utility or character of a data set must be controlled. The system evaluator should identify known constraints on the use of data in support of the system evaluation and plan to handle the constraints as required. Examples of constraints are data from a model that do not play realistic hostile or friendly air defense, data obtained from a single environment, data from immature software, logistics data limited to realistic maintenance below direct support, and data from crews that have not been cross-trained. The system evaluator includes a discussion of whether the constraints will be handled judgmentally or with formal analysis (specify technique), and clarifies the extent to which the impact of constraints is likely to be remedied.

Section V

System Evaluation Reporting

5–25. System evaluation requirements

The objective of CE is to provide periodic reports throughout a system's acquisition life cycle. The system evaluator provides periodic assessments of the system's developmental growth and progress to decision makers, MATDEVs, logisticians, trainers, CBTDEVs, and other acquisition team members. At MS DRs, the system evaluator provides an independent system evaluation of the system's operational effectiveness, suitability, and survivability.

5–26. System-level reports

The SER (or SA) documents findings and recommendations throughout the life cycle of a system. The SER and SA are system-level reports that integrate the information from various event-level reports into an overall assessment of the system. These reports are provided to the MDA for all programs and to OSD for T&E oversight programs. Figure 5–4 depicts an example of the system-level reporting process.

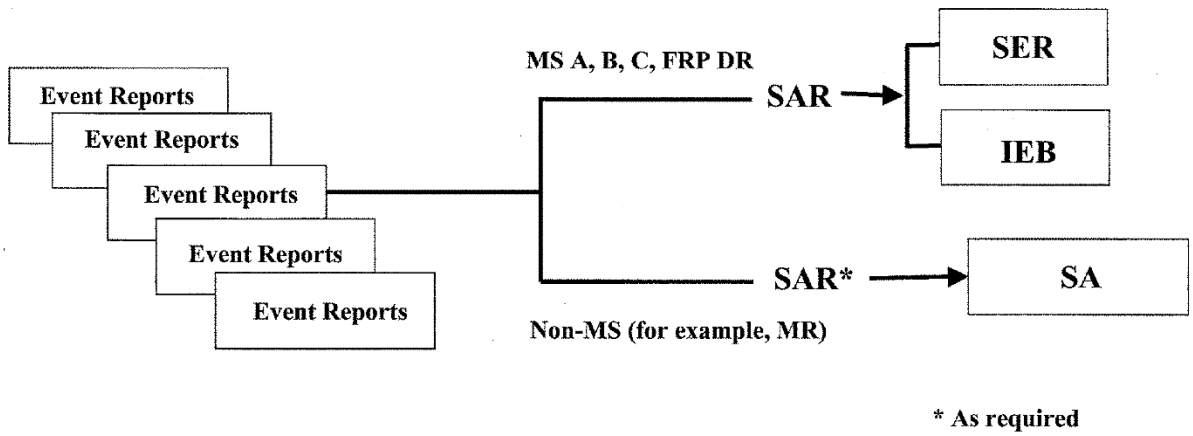


Figure 5–4. System-level reporting process decision

a. System evaluation report. The SER documents the independent system evaluation findings and recommendations regarding a system's operational effectiveness, suitability, and survivability. It is provided at each milestone supported by a safety assessment report that provides the detailed analyses to support the evaluation.

(1) Provides the decision authority with an independent evaluation of the system's performance and operational effectiveness, suitability, and survivability at each MS. When writing the SER, keep in mind the milestone that the evaluation is supporting. A system that has good potential for meeting requirements may be acceptable at MS C but may, or may not, be acceptable at FRP DR when demonstrated results, not potential, are important.

(2) The SER is a stand-alone document and uses all credible data sources.

(3) The safety confirmation is always appended to the SER.

(4) The SER follows the content requirements of the SEP and includes introduction, which includes test limitations and impacts, findings and analysis, and recommendations. Detailed formats may be obtained from ATEC.

(5) The SER is principally written by the system evaluator.

b. System assessment. The SA provides an assessment to date for non-MS decisions (for example, materiel release) and at any point when requested by the MATDEV or the decision maker. It provides an assessment of the progress toward achieving system requirements and may address a subset of the overall evaluation issues. The SA may be based on a single event or a series of events, and the scope of the issues to be addressed is flexible because it may or may not cover all aspects of effectiveness, suitability, and survivability. The SA may identify needed modifications and provide information on tactics, techniques, doctrine, organizations, and personnel requirements. The SA is principally written by the system evaluator and always includes a safety confirmation as an appendix.

c. System analysis report. A system analysis report (SAR) may be prepared in support of the SER or SA if more detail is required. The SAR provides the analysis supporting the system evaluation in enough detail to allow anyone to reconstruct the data and perform additional analyses. It includes in-depth analyses, causality investigations, and diagnostic excursions. The SAR—

(1) Is principally written by the system evaluator.

(2) Accounts for all issues and measures contained in the SEP when the SAR supports a SER.

(3) Provides the analysis supporting a SA only when the analysis is too detailed for inclusion in the SA.

(4) Accounts for only those issues and measures contained in the SA when the SAR supports a SA.

d. Independent evaluation brief. The system evaluator prepares an independent evaluation brief (IEB) based on the SER and/or SA. The system evaluator presents the IEB to the PM or MATDEV, CBTDEV or FP, and DR body (DAB, Information Technology Acquisition Board, Army Systems Acquisition Review Council, or in-process review panel). The briefing summarizes the SER submitted to the milestone decision and contributes to recommendations by the milestone DR body to the decision maker, as well as to management decisions by the milestone DR body. The IEB—

(1) Follows the same outline as the SER.

(2) Summarizes the information contained in the SER in a briefing format.

e. Emerging results brief. The decision to release emerging evaluation results is made by the T&E activity commander on a case-by-case basis. The system evaluator may be required to provide emerging results immediately after a key event (for example, in order to provide information to various DR organizations when there is not sufficient time to wait for the final SER or SA). The system evaluator develops the emerging results brief (ERB).

f. Safety confirmation. Prior to a milestone decision or a materiel release decision, a safety confirmation is provided to the decision makers as part of the SER and/or SA. The safety confirmation provides the safety findings, states whether the specified safety requirements are met, and addresses the risk of proceeding to the next phase of the acquisition cycle. The safety confirmation is provided by the U.S. Army Developmental Test Command (DTC). (See app N.)

5–27. Event-level reports

For each test event that supports the system evaluation, a test report is completed. The report may be called by different names depending on the type of event. Test report formats may be modified to accommodate any peculiar circumstances associated with the event. The test report should fully document the activities and results of the test. The test activity that conducts the test event will prepare, approve, and publish the test report in coordination with the T&E WIPT. (See chap 6.)

a. Test incident report. TIR data are prepared by the test organization (Government or contractor) to provide the results of any incident occurring during testing, to report the results of subtests, and to serve as interim reports. TIRs are reported by both DTC, U.S. Army Operational Test Command (OTC), and other T&E activity through the ATIRS database and include corrective action data, if required. ATIRS is administered by the U.S. Army Aberdeen Test Center (ATC) located at Aberdeen Proving Ground, Maryland. (See app V.)

b. Developmental, operational, and live fire test reports. Developmental, operational, and live fire test reports are addressed in chapter 6.

5–28. Source Selection Evaluation Board

The Government developmental tester and system evaluator will be involved in the acquisition requirements package preparation process and can be an advisor to and may, if appropriate, participate as a member in the Technical Evaluation/Source Selection Evaluation Board. The early involvement of testers and the system evaluator in the acquisition requirements package process and Source Selection Evaluation Board is necessary and is consistent with the Army's CE concept.

Chapter 6
Testing

Section I
Introduction

6–1. Overview of testing
This chapter provides procedural guidance for developing strategies for the testing of all acquisition programs. The primary objective of testing in support of the acquisition process is to provide data to identify and resolve technical, safety, and logistical issues and to verify the attainment of operational goals and objectives. The structuring and execution of an effective testing program is absolutely essential to the acquisition and fielding of Army systems that meet the user's requirements.

6–2. Philosophy of testing
a. Extent. The need for testing is based on the question, "What don't we know that we need to know that can only be obtained from testing?" Testing is conducted only to the extent necessary to provide the answer. Although the time and resources expended on testing are only a small portion of the complete acquisition life-cycle costs, the influence of testing is significant. Experience has demonstrated that where tests have been eliminated or reduced, deficiencies in the system have been overlooked, only to surface after deployment, resulting in expensive and time consuming modifications. Where testing has been adequate and complete, systems have gone to production and deployment sooner than anticipated, thus saving time and money, and with favorable results reflected in the field. All T&E WIPT members must work to avoid unnecessary duplication of testing efforts.

b. Principles. Testing is conducted by applying objective principles to provide data in support of an impartial system evaluation/assessment. Adherence to these principles is necessary to ensure valid estimates of a system's expected operational effectiveness (including survivability and vulnerability) and operational suitability (compatibility, interoperability, RAM, logistic supportability, safety, health, human factors, and trainability). While it is difficult to state established principles simply, they may be summarized in three terms: adequacy, quality, and credibility.

(1) *Adequacy.* The amount of data and realism of test conditions must be sufficient to support the resolution of the COIC and AI.

(2) *Quality.* The test planning, control of test events, and treatment of data must make the information clear and accurate.

(3) *Credibility.* Test conduct must be objective. OT data handling must be separated from external influence and personal/organizational self-interest.

6–3. Waivers of approved testing
DT and OT that are specified in the approved TEMP must be conducted unless a waiver has been obtained from the TEMP approval authority. Policy for waiver requests can be found in AR 73–1.

6–4. Testing of commercial items and non-developmental items
DT and OT requirements should be tailored to each specific system. DT and OT should be conducted at a minimum to verify integration and interoperability with other system elements. Additional T&E, as appropriate, should be conducted to evaluate and control risk. For more information, see paragraph 5–5*b* of this pamphlet. The following provides general guidance, not rigid requirements, of the testing activities appropriate for commercial items, to include COTS and NDIs options:

a. Commercial items or NDI to be used in the same environment for which they were designed (that is, no development or modification of hardware or software is required) will normally not require DT before the MS B decision; however, available data should be sufficient to assess safety, RAM, performance, producibility, supportability, and transportability. The TFT may be conducted to support the MS decision. When the production contract is awarded to a contractor who has not previously produced an acceptable finished product and the item is assessed as high risk, a PVT is required and a LUT may be required before materiel release.

b. Commercial and NDI items that require some modification of hardware or software (for example, militarization or ruggedization) may require a TFT unless the decision authority documents that further testing is not required. A PQT is required if feasibility testing results in the necessity for fixes to the item. To support materiel release, a PVT is required, and a LUT may be required.

c. A research and development effort is required for integration of commercial items and NDI subsystems, modules, or components that contribute to a materiel solution. Systems engineering, software modification, and testing are required to ensure the total system meets user requirements and is producible as a system. A TFT may be required in a military environment. A system-level PQT is required, while hardware and computer software integration tests and/or a LUT may be required. If the PQT or LUT identifies required fixes, a PVT is conducted to address only those parameters that are still in question. If the PQT and/or LUT are completely successful, the PVT may take the form of a first article test (FAT). The PQT and PVT should be similarly designed.

d. Emphasis should be given to logistics support when acquiring commercial items and NDIs. Maximum use will be made of existing commercial support, and existing data should be used whenever possible. A logistics demonstration (LD) or supportability test should be considered when the envisioned military support concept differs from the existing commercial support concept and when no data exist to confirm adequacy of the proposed concept.

e. Some follow-on testing of the commercial item or NDI may be required to verify the adequacy of corrective actions indicated by the PVT.

f. Serious consideration should be given to E3 and RF spectrum supportability when acquiring a commercial item or NDI for worldwide deployment and fielding. Commercially available spectrum dependent equipment may not be frequency supportable in certain international regions and every sovereign nation. Host nation spectrum management approval is required prior to fielding and operations.

g. The OT can provide data not obtainable through other sources (for example, M&S and DT) or may be used to validate previous analytical efforts. It is applicable for all development systems, including commercial or NDI and system changes, unless waived (see AR 73–1) or not required by the TEMP or the system's approved acquisition strategy.

6–5. Testing of clothing and individual equipment

Clothing and individual equipment (CIE) is a collective term that includes personal, optional, and organizational clothing, and individual equipment (usually listed in CTA 50–900 or CTA 50–970) that is not an integral part of the design and operation of an equipment item. AR 70–1 and DA Pam 70–3 govern CIE acquisition. The overall philosophy and process are described in AR 70–1, except that the Army Clothing and Equipment Board and the Clothing Advisory Group recommend items for approval by the Vice Chief of Staff, Army.

a. Upon procurement of a CIE item, Government initial production testing should be conducted to certify the specifications so that future procurements and the Defense Logistics Agency's quality control are effective. T&E management documents for the acquisition of CIE are the same as those required for materiel and C4I/IT systems acquisition acquired under the auspices of AR 70–1 (that is, TEMP, SEP, EDP, detailed test plan (DTP), test report, and SER).

b. Requirements for OT of CIE are based on the COIC associated with the program.

6–6. Joint test and evaluation

The OSD-directed Joint Test and Evaluation (JT&E) Program brings two or more Services together to evaluate technical or operational concepts, interoperability, testing methodologies, and joint military mission capabilities; improve M&S; and provide feedback to the acquisition community, as directed in a formal charter from the Director, Strategic and Tactical Systems, USD (AT&L). An annual OSD nomination process, a feasibility study process of 8–10 months, and a testing process of 3 or more years support the JT&E Program.

a. Army nominations are solicited annually, in the March-April timeframe, for consideration by an Army Nomination Board that convenes in January of the following year. The Army's participation in the JT&E Program is managed by DCS, G–8–FD. The selection of suitable nominations to become feasibility studies and the selection of completed feasibility studies to become chartered OSD-directed JT&E is determined primarily by the recommendations of the Senior Advisory Council (SAC), co-chaired by the Director, Strategic and Tactical Systems of USD (AT&L) and DOT&E. The Army's SAC representative is from DCS, G–8–FD, reviews the Army Nomination Board's prioritized recommendations, and approves the Army nominations submitted to OSD to compete for entry into the feasibility study phase.

b. After being directed by OSD, the lead Service will conduct a joint feasibility study over the next 8–10 months to assess the need and feasibility for executing the JT&E, expand and refine the nomination test concept, prepare a feasibility study report that specifies resource requirements for OSD and the Services. During this phase each feasibility study will be reviewed by an OSD Technical Advisory Board three times. The Technical Advisory Board provides technical guidance and makes feasibility recommendations to the SAC. Upon completion of the feasibility study and favorable review by the SAC, the JT&E candidate may be recommended for charter as a JT&E.

c. JT&E charters designate a "lead Service" and one or more "supporting Services." OSD is the primary source of funding for a chartered JT&E. The Services provide office facilities, personnel to staff the Joint test force, test support,

and other personnel and equipment to participate in test events, consistent with their involvement as defined in the approved feasibility study.

d. DCS, G–8–FDR manages Army participation in the JT&E Program and provides a member to the JT&E Planning Committee. The JT&E Planning Committee is a working-level body that meets to review nominations, exchange information on Service positions and prepare nominations for presentation to the SAC. DCS, G–8–FD also provides the Army's voting member on the SAC. For chartered JT&E, ATEC maintains manpower authorizations on the U.S. Army Element Joint Test Activities' table of distribution and allowance, requisitions personnel to staff the full-time test directorate positions, budgets for the Army's participation and lead Service costs, and coordinates Army-wide JT&E support requirements through the Test Schedule and Review Committee (TSARC) process. All personnel and resource actions regarding the JT&E Program are reviewed and approved by DCS, G–8–FD. ATEC provides technical T&E advice through test document reviews, technical advisory groups, general officer steering committees, and membership on the OSD JT&E Technical Advisory Board.

e. For more information on JT&E, see http://www.jte.osd.mil/, DoDI 5010.41, DoD 5000.3–M–4 (JT&E Procedures Manual), and AR 73–1.

f. The memorandum of agreement among the four OTA commanders dealing with JT&E can be found by accessing http://www.hqda.army.mil/tema.

6–7. Multi-Service operational test and evaluation

a. A JROC approval of a requirement that impacts more than one DoD component normally initiates an acquisition and, thus, multi-Service tests. Tests are conducted for systems being acquired by more than one DoD component or for systems that interface with equipment of another Service. OSD designates a lead Service to prepare the T&E plan and final report on the system. However, resource planning and support are the same as for any other Army OT. Requirements are documented, coordinated, and prioritized in the TSARC and FYTP processes. ATEC is the focal point for coordination of Army resources to support multi-Service T&E. This includes budgeting for the testing necessary to accomplish assigned test objectives and for participation of Army personnel and equipment in the entire test program.

b. DT for acquisition programs being developed and tested jointly follows the testing procedures of the designated lead Service. All program documents, including the TEMP, and other T&E plans and reports, are developed by the lead Service. (See AR 73–1.)

c. The memorandum of agreement among the four OTA commanders dealing with multi-Service operational T&E can be found by accessing http://www.hqda.army.mil/tema.

6–8. Testing in support of system changes

T&E of system changes (that is, modifications, upgrades, and horizontal technology integration) will be conducted to verify the extent of the change and its operational impact on mission accomplishment.

a. The MATDEV, in coordination with the T&E WIPT, determines the DT requirements. (See para 5–5 and fig 5–1.)

b. Requirement for OT is based on the COIC and further outlined in the TEMP and SEP.

6–9. Testing in support of reprocurements

Reprocurements of materiel and C4I/IT systems may require DT and OT, depending on the level and type of configuration changes (see AR 73–1). Testing requirements to support reprocurements of non-tactical C4/IT systems generally follow those options outlined for information system changes. Changes that apply to all types of systems and may require DT and/or OT to be conducted as follows:

a. The system being procured is a different make and model from the original system or is being produced by a different manufacturer.

b. The system has had a break in production of more than 2 years.

c. The system's operational capability envelope has changed.

d. Testing types for reprocurements are—

(1) Pre-FRP DR tests include PQT, PVT, LUT, and IOT.

(2) Post-FRP DR FOT is conducted rarely and only as needed for reprocurements.

(3) TRADOC may use a CEP test to redefine requirements for reprocurements to include testing in support of NDI market investigations.

(4) TRADOC may use FDT/E as required for system reprocurements.

6–10. Foreign comparative testing

The FCT testing program recognizes the value of NDI items of allied and friendly nations to satisfy DoD Component requirements or correct mission area shortcomings. The program is dependent on user interest and a valid operational requirement for a developed foreign item with good procurement potential. FCT can eliminate unnecessary testing. A favorable evaluation, usually based on DT data, of the foreign item is also required.

6–11. Testing in support of limited procurement

OT is conducted and can be expedited to support LP prior to materiel release to the first unit equipped if the urgent requirement permits. The ATEC's OTC participation in LP procurement can cover a spectrum of involvement, for both war and non-wartime urgent procurement. OTC participation in LP procurement can provide a test report based on results of a quick reaction LUT. ATEC's DTC safety confirmation will be provided to support LPs.

6–12. Testing in support of the combat and training development process

FDT/Es are conducted with troops under field conditions. A FDT/E supports force development and materiel development processes by examining the effectiveness of existing or proposed concepts of doctrine, training, logistics, and materiel. A FDT/E may be conducted during any phase of the materiel acquisition process. It may be related to, combined with, or used to supplement OT. During the requirements formulation effort, FDT/E may be used to determine essential and desirable capabilities or characteristics of proposed systems. Prior to MS B, a FDT/E can be used to assist in refining concepts of employment and DOTMLPF, or in lieu of OT when operational issues are adequately addressed. FDT/E also includes field experiments designed to gather data through instrumentation to address a training development problem or to support simulations, models, wargames, and other analytical studies. Requirements for FDT/E may also be generated by the results of combat developments, training developments, or training effectiveness analysis, testing, and studies.

a. FDT/E used to support the acquisition process should be included in the TEMP.

b. The organization for which the FDT/E is being performed provides the general requirements that establish the FDT/E objectives. These are normally stated in terms of operational issues and criteria, test or experiment objectives, or data requirements for subsequent analysis. Regardless of the form, these requirements are used as the basis for the design of the FDT/E.

c. Design of the FDT/E is documented in a SEP and/or an EDP.

d. FDT/E may be structured to provide necessary information to support development of JMEMs. Such needed information may be in the form of weapons characteristics data (for example, blast and fragmentation), weapons employment/engagement scenarios/conditions, and in the form of operational suitability.

6–13. Acquisition requirements package and Source Selection Evaluation Board

The Government developmental tester, operational tester, and system evaluator may be involved in providing technical information or advice to the acquisition requirements package and Source Selection Evaluation Board. Testers and evaluators are usually not Source Selection Evaluation Board members, and thus they do not make selection recommendations or decisions.

6–14. Combined or integrated testing

The increased emphasis to streamline the acquisition process requires the T&E community to always consider combining or integrating testing. A combined developmental test and operational test (DT/OT) is a single event that produces data to answer developmental and operational system issues. A combined DT/OT is usually conducted as a series of distinct DT and OT phases at a single location using the same test items. For the case where a single phase can be used to simultaneously meet developmental and operational issues, this testing will be referred to as an integrated DT/OT. Combined DT/OT and integrated DT/OT are encouraged to achieve time, cost, and resource savings. However, they should not compromise DT and OT objectives. The execution strategy for an integrated DT/OT event is based on the requirements of the program. The testers and system evaluator, in coordination with the T&E WIPT, must look objectively at the expected outputs to determine the worth of the event to the overall information and data needs for evaluation of the system.

a. Each test event (whether separate, combined, or integrated; a model; a simulation; or a model or simulation used in conjunction with live testing) has an appropriate role to play in providing data/results for evaluation of a system's performance, safety, and operational effectiveness, suitability, and survivability. The requirements of the developmental or operational environment coupled with statutory and regulatory requirements will usually require some degree of separate DT early in the program and separate OT late in the program. However, an integrated T/SES will be

developed when it is judged to be the most effective and efficient event to support the evaluation requirements. The MATDEV, along with the T&E WIPT, must assess the technical risks associated with choosing this approach.

b. Specific types of DT and OT are defined in AR 73–1. How tests might be combined or integrated to provide all the necessary data for the system evaluation is always tailored to the specific program while recognizing that there are many possibilities within these guidelines.

(1) In the early phase of a program, tests will be primarily focused on technical and performance evaluation to establish technical validity, resolve design problems, and support development of a mature production representative design. At this stage, much of the test activity may not directly address operational issues. The goal of test integration at this stage is to assure that operational issues are considered in the resolution of technical problems and corresponding design changes. At the other end of the spectrum, IOT should be conducted with a mature production representative system with all technical hardware and software problems resolved. Between these two extremes is the greatest opportunity to achieve economy and efficiency through effective test integration that will address as many developmental and operational issues as possible with a single, comprehensive, and integrated test effort.

(2) A combined DT/OT is conducted as a continuum, with distinct entrance and exit criteria. A combined DT/OT need not be a simultaneous event. A combined DT/OT event is typically a series of distinct DT and OT phases. The DT phase focuses on generation of technical test data under control of the developmental tester and may permit MATDEV and system contractor involvement. The OT phase focuses on generation of operational test data under the control of the operational tester with typical user personnel in an appropriate operational environment using production representative systems. MATDEV involvement is limited and system contractor involvement is normally prohibited during this phase unless contractor logistical support is part of the Army's fielding plan.

(3) Integrating DT/OT into a single phase requires that normal DT and OT requirements will not be compromised and that any statutory or regulatory requirements for MATDEV and system contractor involvement are maintained.

c. There are many issues that must be considered when combining or integrating tests, such as—

(1) An event taking place pre-MS C may combine or integrate a TFT, an EDT, or a software development test with an EUT. A post-MS C event might be a PQT combined or integrated with a LUT. An integrated test will not normally include an IOT for a MDAP. A post-FRP event may be a PVT combined with a FOT.

(2) Integrating the TFT/EUT is most appropriate for events conducted before MS B when the operational requirements are not generally subject to restrictions required for tests in support of the production decision. An additional benefit is that increased system contractor involvement can be included to assist both the DT and OT elements in the test to better understand, maintain, and explain performance of the system. Limitations for this type of event would increase if the TFT/EUT was used for a selection among candidates for further development or if the system complexity or risk required extensive safety requirements for user personnel.

(3) Integrated testing following MS C must be considered carefully. Considerable resources are normally required to bring all the elements necessary for a LUT into position at an appropriate location. Any significant risk that the system may not be ready for OT requirements (such as potential user safety risk, inability to properly train user personnel, or other possible shortfalls in meeting the OT requirements for the event) should be carefully considered. OT is normally conducted at the home station of the designated user unit. Consideration of whether the DT objectives can be achieved in the typical operational environment must be considered. After the FRP decision, integrated testing can be performed, but the same issues must be considered. A PVT/FOT event is possible after a careful review of the requirements.

(4) Combined DT/OT can generally be conducted within all phases of the acquisition program cycle. The key limitation is generally the required location for the combined test. As stated, most OTs are performed in the typical operational environment and would require DT elements to test at that site. Additional requirements are the availability of an appropriate safety release for the personnel operating the system in the OT phase, and adequate confidence that the system would be ready to continue into the OT phase following the DT. DT typically leverages matrix resources and specialized, fixed facilities optimized to reduce time and cost while ensuring data accuracy. Any situation that would prohibit continuance of the OT phase would result in loss of the resources assembled for the phase. Subsequent reschedule of the testing would require additional resources and add to the overall cost and timelines for the program.

(5) Additional considerations when developing an integrated test strategy include—

(a) Various degrees of integration can be achieved by using M&S in conjunction with live testing. (See para 5–21.)

(b) Using the same data collectors for both DT and OT. This ensures the data disseminated in the TIRs are consistent, making it easier for the evaluator to understand and use the data.

(c) Using the same military test participants. This will provide OT Soldiers more experience on the test systems, ensuring that the test players are more representative of those who would use the mature, fielded system. It will also provide early user influence in the design allowing the hardware to mature sooner. Even so, the system evaluator must be aware of the specific level of training so as not to create an unwanted "Golden Crew" situation.

(d) Using the same instrumentation. This will eliminate redundant development and ensure that the instrumentation developed will meet all requirements.

(e) Using common questionnaires and data forms to facilitate data handling and summarization by the evaluators.

(f) Considering the possibility of collecting OT data during DT.

(6) Section 4171 of Title 10 of the USC, the Defense Acquisition Guidebook, and AR 73–1 all set limitations on system contractor involvement in OT events. Statutory and DoD requirements exist for those systems designated as MDAPs, that is ACAT I and II. Army policy applies the same restrictions to all Army acquisition programs.

(a) Army policy requires that system contractor personnel will not—

1. Participate in operational events except to the extent that they are involved in the operation, maintenance, and other support of the system when it is deployed.

2. Participate in collecting, reducing, processing, authenticating, scoring, analyzing, or evaluating operational test data.

3. Attend or be directly involved as members or observers in DAG (see para 6–52), RAM Working Group of the T&E WIPT, and RAM Scoring and Assessment Conferences that address data supporting the system evaluation of their systems. Serving as technical subject matter experts outside of these forums is allowed.

(b) Application of the system contractor involvement limitations can usually be made without undue difficulty in the separate phases of any combined DT/OT. Clear understanding of actions considered permissible during both phases is needed prior to test execution. This will ensure that all concerned understand the constraints and the point at which DT ends and OT begins.

(c) If an integrated test is conducted prior to the LRIP decision, more involvement of the system contractor is permissible because such data are generally not used to support the FRP decision. However, if the data will be used to support the FRP decision, the full restrictions must be considered.

(7) The end result of the combined or integrated DT/OT is information provided to support the system evaluation. A properly structured SEP will normally provide the required data for the evaluation at the various program decision points. The T&E WIPT must consider the most effective and efficient use of testing, including M&S, as an overall component of the strategy. Combined or integrated testing should be considered as one tool to be used but not as the only tool in the toolbox. Separate DT and OT will, in some programs, still provide useful information and data not obtainable in combined or integrated testing. Risks must be carefully considered to ensure that combined and/or integrated testing is not performed under conditions that do not provide usable information.

Section II

Developmental Testing

6–15. Overview of development testing

a. DT is a generic term encompassing engineering-type testing, generally requiring instrumentation and measurements, which is accomplished by engineers, technicians, and Soldiers, as necessary, using instrumented open air ranges, hardware in the loop simulators, installed system test facilities, models, or simulations. It includes technical feasibility testing, engineering development testing (such as capacity, stress, and performance testing; security certification testing, tactical communications, and interoperability testing), software development testing, production qualification testing, production verification testing, and testing in support of post-deployment hardware and software evolution, as well as support to identify and resolve problems revealed during sustainment.

b. DT identifies the technological capabilities and limitations of the alternative concepts and design options under consideration. DT also identifies and describes design technical risks. DT can assist in the design of a system at the component, subsystem, and system level by reducing technical risk prior to transitioning to the next level;

c. DT stresses the system under test at least to the limits of the OMS/MP by "pushing the envelope" to ensure expected operational performance environments can be satisfied. For some systems it may be appropriate to push beyond the normal operating limits to ensure the robustness of the design.

d. DT can address the potential of satisfying operational test and evaluation (OT&E) requirements to the best extent possible by testing in operationally relevant environments (simulated or actual), without jeopardizing DT objectives, to reduce overall T&E redundancy and costs.

e. DT can analyze the capabilities and limitations of alternatives to support cost-performance trade-offs.

f. DT can assess progress toward meeting KPPs and other ORD requirements, COIC, mitigating acquisition technical risk, and achieving manufacturing process requirements and system maturity.

g. DT assesses technical progress and maturity against CTPs, to include interoperability, documented in the TEMP.

h. DT provides data and analytic support to the decision process to certify the system ready for OT.

i. DT, in the case of IT systems, supports the IT systems security certification process.

j. Prior to FRP, DT demonstrates the maturity of the production process through Production Qualification Testing of LRIP assets.

k. DT is conducted throughout the acquisition process to assist in the systems engineering design and development of a system, provide safety verification, and to verify that performance specifications have been met. Plans for DT should be coordinated with a SSP. The goals being increased effectiveness of the systems engineering process as well as implementation of a sound STEP. (See AR 73–1.)

l. DT provides data with which to assess validity of assumptions incorporated in M&S; performance levels of new technologies inserted into prototype hardware; achievement of systems engineering design goals; compliance with CTP; and to identify technological and design risks and determine readiness to proceed to IOT. DT is conducted throughout production to accommodate product acceptance testing necessary because of manufacturing changes allowed by performance based acquisition strategies. If a program experiences technical or operational problems, DT provides a valuable service by helping to identify problems and verify fixes before they seriously affect program cost and schedule. A concerted effort is required by the testers, system evaluator, and the system developer to mature the equipment technically and properly test it before transitioning to OT or the production processes. DT substantiates the achievement of contractor technical specifications.

m. DTs are designed to subject the system or its components, both hardware and software, to stress levels commensurate with those to which the mature system will be subjected in all operating environments. To the degree feasible, tests should be conducted in accordance with the OMS/MP. If required, DT may subject the system to stress levels that will estimate the outer limits of the operational envelope. DT determines the system safety, technical performance, MANPRINT, human factors performance, reliability, survivability, ILS, interoperability with associated equipment, and the integrity of the equipment. A safety release (based on the results of DT) is required before involving Soldiers in any test. (See paras 6–64 and 6–65.)

6–16. Developmental test planning

a. As chair of the T&E WIPT, the PM or MATDEV works with its members to structure a T&E program concurrently with the acquisition strategy. (See chap 2.) Consideration must be given to DT over the system's entire life cycle. Program planning documents are a source of information to assist the T&E WIPT and the developmental tester in identifying future resource requirements (for example, personnel, funds, facilities, and instrumentation).

b. Before each acquisition decision milestone, sufficient DT and system evaluation must be done to demonstrate reduced acquisition risks and to estimate the capability of the system to meet the CTP. DT programs are structured to provide sufficient data to allow evaluation of issues regarding, but not limited to, safety; performance; RAM; and MANPRINT considerations. The system evaluator provides the MDA with information that addresses the CTP, specifying which parameters have been designated as exit criteria by the MDA. Exit criteria are the specific minimum requirements that must be satisfactorily demonstrated before the program's next acquisition decision milestone can be scheduled.

c. DT is planned and conducted to take full advantage of the existing investment in DoD ranges and other test facilities, whenever practical. Agencies with requirements for developmental, production, or post-production testing of military materiel must use DoD Major Range and Test Facility Base (MRTFB) activities and other DA test facilities instead of establishing in-house capabilities or contracting for testing services. Exceptions will be justified in the TEMP (see AR 73–1 and the Defense Acquisition Guidebook). DT is coordinated with ATEC's DTC or the SMDC to maximize the Army's capital investment in its MRTFB facilities. This coordination takes place before program initiation and facilitates the generation of DT requirements as well as determining the extent and nature of contractor services, if required.

(1) The DoD MRTFB is an aggregation of test activities, facilities, ranges, and equipment designed to provide DoD with the best overall military T&E capability. See DoDD 3200.11 for a summary of capabilities of all DoD MRTFBs. The MRTFB is operated and managed under uniform reimbursement policy. DoD test customers utilizing the MRTFB are required to pay only those costs that are directly identified to the test. The indirect or overhead costs are funded by the MRTFB activity's parent command (see AR 73–1).

(2) The MRTFB and other test and research and development facilities are capital investments designed to provide comprehensive testing capabilities that support all materiel acquisition programs. These facilities have unique capabilities and expertise and offer significant cost benefits to customers.

(3) DA MRTFB activities are U.S. Army Yuma Proving Ground (YPG), AZ; U.S. Army Dugway Proving Ground (DPG), UT; ATC (located at Aberdeen Proving Ground, MD); U.S. Army White Sands Missile Range (WSMR), NM, including U.S. Army Electronic Proving Ground (EPG) (located at Fort Huachuca, AZ); U.S. Army Ronald Reagan Ballistic Missile Defense Test Site (RTS), U.S. Army Kwajalein Atoll (USAKA), Wake Island; and High Energy

Laser Systems Test Facility (HELSTF), WSMR, NM. Appendix R of this pamphlet contains a brief description of the DA test capabilities, including the DA MRTFB activities.

6–17. Developmental testing of non-tactical C4/IT systems

DT of non-tactical C4/IT systems in support of system evaluation includes software development tests, software PQTs, and tests in support of either PPSS or PDSS.

a. Software development tests are an inherent part of development and are conducted by the developer of the system's program at the unit, module, and integration level.

b. PQTs are conducted at the system-level on target hardware by a Government developmental tester prior to the FRP DR. A PQT is conducted after the system security certification settings and mechanisms have been implemented and frozen so as to not invalidate the qualified baseline. Tests during PDSS consist primarily of modifications and maintenance of software. (See para 5–15*e*(10) and app Q.)

c. System-level DT is conducted at stress levels representative of data volumes expected to be encountered under the most extreme circumstances (for example, deployment surge, wartime operation with full force structure participation, and year-end closeout processing). DT will be structured to estimate the outer limit of the system's operational envelope.

6–18. Mission of the developmental tester

a. The developmental tester plans, conducts, and reports the results of DT. As a T&E WIPT member, the developmental tester assists in designing an effective DT program. DT reports are provided, as appropriate, to the MATDEV, the system evaluator, other members of the T&E WIPT as authorized by the MATDEV, the milestone DR body, and, for ACAT I and other OSD T&E oversight programs, to OSD through the DUSA (OR).

b. DT and associated production testing on Army materiel systems are normally executed by U.S. Army DTC unless otherwise designated in the TEMP. Exceptions for DT may be non-tactical C4/IT systems assigned to the U.S. Army Communications-Electronics Command (CECOM) (by the CIO/G–6), U.S. Army Medical Command (USAMEDCOM), United States Army Intelligence and Security Command, SMDC, and U.S. Army Corps of Engineers.

6–19. Testing for commercial entities

The Army is authorized to provide testing services to commercial concerns (AR 73–1). Policy dictates the rates charged as follows:

a. When a contract between a private industry and a DoD agency already exists and includes language authorizing test support/services from Army test facilities, Army test agencies are authorized to charge DoD rates. Research, development, test, and evaluation (RDT&E) contracts should include the following specific language: The contractor is authorized to obtain test support/services at DoD rates from Army test ranges as Government-furnished services. Under these circumstances, DoD rates be charged to the Defense contractor provided the Army test agency receives a copy of the contract containing the required language. The request for test and cost estimate as well as payment of test funds may come from private industry. If the funds are received at the test agency directly from private industry, a contract must be signed by both parties and in place prior to testing. A prospective contractor who is preparing to bid on a Government contract that includes a requirement for testing may request and receive a cost estimate for the test from the Army test agency.

b. Test services may be provided by Army facilities for private industry when no related acquisition contract exists. The Fiscal Year (FY) 94 Defense Authorization Act amended Title 10 of the U.S. Code to provide increased access to DoD T&E facilities by commercial users. DoD guidance requires MRTFB facilities to charge commercial customers all direct costs associated with the test but permits the MRTFB commanders to determine the indirect costs to be charged as deemed appropriate.

6–20. System contractor participation in developmental testing

DT objectives include verifying system maturity, logistic supportability, human factors, security features, and system safety. Therefore, testing is designed to find, analyze, and fix problems and verify the solutions. Meeting these objectives requires engineering level involvement of and discussions with system contractor personnel.

a. The degree and nature of system contractor involvement in DT that is not inherent to development is agreed upon by the MATDEV, the system evaluator (when the DT supports the system evaluation), the Army test agency, and other agencies or organizations, as applicable. These agreements are reached through the T&E WIPT process and are then communicated through the contractual requirements. Developing these agreements early will help to ensure that test data will be usable for the system evaluation.

b. System contractor involvement may range from total control during testing that is inherent to development (that is, unit, module, and integration) to no direct involvement, to providing spare parts and technical advice during the conduct of a DT, to performing the entire spectrum of DT. When the system contractor is directly involved in the conduct of DT at an Army test facility, special consideration may be required to address security, personnel safety, and the protection of competition sensitive test data. Special consideration should be given to control of Web based developmental software that is under test, where the application server is under control of external elements such AKO portals, and developers only have write capability access to the application. Consideration should be given to the use of a combined Government/contractor DT team, especially when the system contractor will perform the testing. Use of the DT team provides for Government participation in the development of the system contractor test plans. The test results are reported by the system contractor and verified by the Army test personnel, thus avoiding duplication of testing.

c. The degree of system contractor involvement in the RAM scoring and assessment conferences (see app K) dealing exclusively with DT and system evaluation will, likewise, be determined by the MATDEV and system evaluator in coordination with the T&E WIPT. System contractor personnel, in general, should not be physically present during the formal voting/scoring and assessment period. However, the presence of system contractor personnel may be allowed during formal scoring at developmental scoring conferences if it is considered necessary for proper information flow. At anytime in this process, a system contractor may be asked to appear to answer questions but should leave after the questions have been answered. Exceptions to this guidance are discussed in the following paragraph.

d. In those cases where DT and OT are planned and described in the TEMP to be combined or integrated under similar conditions (for example, OMS/MP, stresses, environmental conditions, test support, and fixed or same configuration), DT results will be combined with OT results in support of the system evaluation. The parameters for system contractor involvement must be carefully coordinated initially at the T&E WIPT and throughout the T&E process to ensure the MATDEV's contractual obligations and the system evaluator's statutory restrictions are met. (See AR 73–1.)

6–21. Developmental test data confirmation

The purpose of test data confirmation is to ensure the widest possible use of data. The T&E WIPT first determines whether or not a need exists to confirm certain test data. A review of each test is performed and the criticality of the use of the data is assessed. This determines which tests require confirmation so the data generated can be used for system evaluation purposes. Test data confirmation is determined by the T&E WIPT.

a. Acceptability of data. In those instances when a particular facility's ability to provide acceptable data is in doubt, the Government developmental tester, the MATDEV, and the independent system evaluator, if appropriate, inspect the facility to verify acceptability of data. For this reason, it is essential that the T&E WIPT review and coordinate on the T&E portion of the RFP prior to its issuance. The following factors should be considered in determining the acceptability of the test data that will be generated:

(1) Ranges, courses, test apparatus, and support equipment available to tester.

(2) Laboratory facilities, instrumentation, and calibration available to tester.

(3) Test personnel experience and expertise, test procedures, and data collection and reporting procedures used by tester.

b. Government monitoring. In those instances when the test data from a particular source or procedure would not otherwise be acceptable, the independent system evaluator may require the test to be conducted by Government test personnel or that the data be validated through monitoring by Government test personnel.

c. Confirmation process. Once the confirmation process has been established, the MATDEV relies upon the Government developmental tester to provide assistance in contractual proceedings. Prior to bid solicitation, the MATDEV—

(1) Provides the T&E portion of the RFP to T&E WIPT members for coordination and to confirm test data acceptability.

(2) Provides to prospective contractors in the RFP, the option of using Government test services, funded directly by the MATDEV. This provides flexibility to the contractors and gives the T&E WIPT a known source of acceptable data, should other sources prove unacceptable. (See AR 73–1.)

d. Contract requirements. To help ensure acceptability of test data, contracts specify that the contractor—

(1) Provide a test plan to the MATDEV for T&E WIPT coordination prior to testing.

(2) Report test incidents to the MATDEV and system evaluator.

(3) Report the corrective actions taken in response to test incidents to the MATDEV and system evaluator.

(4) Provide a test report to the MATDEV and system evaluator. If contractor test data will be used to satisfy certain technical requirements, a copy of the contractor test report should be provided to the Government developmental tester by the MATDEV.

6–22. Developmental testing and the Army Logistician

The logistician works closely with the acquisition community through cross-functional IPTs, Integrated Logistics Support Management Team (ILSMT), T&E WIPT, and other program reviews to ensure DT provides data for a continuous assessment of logistics support program management and execution. The Army logistician contributes to the identification and resolution of logistics issues while reviewing and assisting with the development of program management documentation and preparation of DT event design requirements. The Army logistician assists the acquisition community with selected analyses using approved models to support repair or discard decisions, level of repair decisions, selection of secondary items to be stocked, and other cost benefit analyses. For class VIII medical materiel, the Army logistician is the USAMEDCOM.

6–23. Developmental test types

DTs are categorized as reflected in AR 73–1. A definition and brief description of the types of DT that can be performed throughout the system's acquisition life cycle is described below. The test types are separated into the pre-FRP, production, and post-production phases. The software tests defined here are software development test, software qualification test (SQT), and PDSS.

a. Pre-full-rate production developmental testing. DT can be conducted during the period before program initiation and prior to the FRP decision using funding categories 6.1 through 6.4. (See DoD Financial Management Regulation, Volume 2B, Chapter 5 for information on funding categories.) Pre-FRP DT test types are as follows:

(1) Research efforts conducted during the pre-systems acquisition phase to determine early technical parameters, to support the research of these items, and to provide fundamental knowledge for solutions of identified problems.

(2) A TFT is typically conducted during the concept and technology development phase to assist in determining safety, establishing system performance specifications, and determining feasibility of alternative concepts. Testing identifies and reduces risks in subsequent acquisition phases. This test provides data for the independent system evaluation that supports the SER required for MS B decision.

(3) An EDT is conducted during system development and demonstration to provide data on system limitations and performance, safety, security, NBC survivability, the achievability of a system's CTP, refinement and ruggedization of hardware configurations, and determination of technical risks. The EDT includes the testing of compatibility and interoperability with existing or planned equipment and systems and the system effects caused by natural and induced environmental conditions. An EDT may be conducted at the component/subsystem or system levels.

(4) A production prove-out test is conducted during systems acquisition (that is, post-MS B and before production with prototype hardware) for the selected design alternative. The production prove-out test is usually performed at the subsystem level and provides data on safety, NBC survivability, the achievability of CTP, refinement and ruggedization of hardware and software configurations, and determination of technical risks.

(5) A PQT is a system-level DT conducted post-MS C that ensures design integrity over the specified operational and environmental range. PQT must be completed using LRIP assets, when available. PQT normally uses prototype or pre-production hardware and software fabricated to the proposed production design specifications and drawings. Such tests include contractual RAM demonstration tests required prior to production release. This test provides data for the system evaluation that supports the FRP DR. The objectives of the PQT are to obtain Army confirmation that the design is stable, logistically supportable, capable of being produced efficiently, and will meet the performance/user requirements; assess the inherent performance envelope; meet security requirements, and determine the adequacy of any corrective action indicated by previous tests. PQT may also include tests that are not included in the data package or contract (for example, environmental extremes and test-to-failure) when such tests are necessary to obtain engineering data to verify corrective action or other purposes. PQT may be accomplished in phases (for example, preliminary engineering and specific problem correction). When conducted by the contractor, the PQT is designated PQT–C.

(6) A live fire test is conducted for those weapons systems required by 10 USC 4172 to undergo LFT&E (see chap 5 and app J). The LFT may be conducted as part of or in conjunction with the PQT. The LFT demonstrates battle-resilient survivability or munition lethality. It will provide insights into the principal damage mechanisms and failure modes occurring as a result of the munition/target interaction and into techniques for reducing personnel casualties or enhancing system survivability and lethality. The scope of LFT&E generally will include the building-block approach, progressing from early component-level testing, to sub-system/system level testing, culminating in a series of FUSL live fire tests. (See app S.)

(7) A LD examines the achievement of maintainability goals; the adequacy and sustainability of tools, test equipment, built-in-test equipment, selected test program sets, technical publications, maintenance instructions, troubleshooting procedures, and personnel skill requirements; the selection and allocation of spares and repair parts, tools, test equipment, and tasks to appropriate maintenance levels; and the adequacy of maintenance time standards. The LD is ideally conducted at least 6 months prior to the IOT to allow time to make corrections, if required. It is often convenient to conduct an LD in conjunction with the PQT. The LD may use selected analysis, evaluations, demonstrations, and testing tailored to each acquisition program to demonstrate adequacy of the proposed support concept and programmed support resources.

(8) A software development test covers the full spectrum of tests that are inherent to software development (that is, M&S, unit, module, integration, security, stress, conversion, software certification, and full-up system testing prior to Government testing).

(9) A SQT is a system-level test conducted by the Army developmental tester using live data files supplemented with user prepared data and executed on target hardware. Conversion procedures and special training requirements are introduced as additional elements for V&V. SQT objectives are to have the Government confirm that the design will meet the performance/user requirements and to determine the adequacy and timeliness of any corrective actions indicated by previous testing. System users participate in the technical and functional aspects of the software development test. (See app T.)

(10) Joint interoperability certification testing applies to all Army C4I systems having interfaces or interoperability requirements with other Service systems. This test may consist of simple demonstrations using message analysis or parsing software with limited interface connectivity, or extend to full-scale scenario-driven exercises with all interfaces connected. The CECOM SEC serves as the Army participating test unit coordinator (APTUC), and in that capacity, supports interoperability testing of C4I systems conducted by the Defense Information Systems Agency (DISA), JITC for system certification and recertification. The CECOM SEC APTUC arranges, coordinates, and participates at all Joint interoperability testing with the DISA and coordinates the participation of all Army elements and systems. See JITC Plan 3006, Joint Interoperability Test Plan (JITP), for testing Tactical Data Link (TDL) and U.S. Message Text Format (USMTF) systems located at https://jitc.fhu.disa.mil/index.aspx. The U.S. Army Aviation and Missile Command (AMCOM) Software Engineering Directorate (SED) serves as the aviation, air, and missile defense representative to the Army participating test unit (APTU), provides tactical hardware and systems along with associated sensor simulations in support of interoperability testing, coordinates with PEOs/PMs to schedule interoperability test assets, and prepares the Army aviation, air, and missile defense systems for connectivity into the JITC testing environment.

b. Developmental testing production testing. Production testing is required to verify that the requirements specified in the ORD and production contracts for hardware and software are met. It also provides test data for the SA required for materiel release decision, ensures the product continues to meet the prescribed requirements, and provides a baseline for post-production testing.

(1) The PVT is a system-level test conducted post-FRP to verify that the production item still meets CTP and contract specifications, to determine the adequacy and timeliness of any corrective action indicated by previous tests, and to validate the manufacturer's facilities, procedures, and processes. A PVT will also provide a baseline for the test requirements in the technical data package for post-production testing. The PVT is accomplished during the first limited production or full-scale production contract. This test provides data for the materiel release (MR) decision, allowing the system evaluator to address the adequacy of the system with respect to the stated requirements. Materiel release is accomplished during the first post FRP DR production contract and is repeated if the process or design is significantly changed, if a second source for the system or major components therein is brought online, or if a significant break in production occurs. (See AR 770–2 and AR 770–3.)

(a) The PVT may take the form of a FAT if such testing is required in the technical data package for quality-assurance purposes. This may be required to qualify a new manufacturer or procurements from a previous source out of production for an extended period of time, and to produce assemblies, components, or repair parts that conform to the requirements of the technical data package. Requirements for FATs may be invoked in production contracts by citation of the applicable Federal Acquisition Regulation (FAR) first article inspection and approval clause. When a FAT is specified in a contract, it may not be waived or changed without prior approval of the head of the contracting activity. A FAT may be conducted at Government facilities or at contractor facilities when observed by the Government. Requirements for the FAT should be consistent with those of the PVT.

(b) The PVT may also include tests that are not included in the data package or contract (for example, environmental extremes and test-to-failure) when necessary to obtain engineering data for corrective action verification, to support a materiel release decision, or to meet another purpose.

(c) Follow-on PVT. A follow-on PVT may be conducted on full production models if the production process or design is significantly changed, or to verify the adequacy of corrective actions indicated by the PVT or to determine production acceptability. A follow-on PVT is structured similarly to PVTs.

(2) A comparison production test (CPT) is a test of randomly chosen samples from production and is conducted as a quality assurance measure to detect any manufacturing or quality deficiencies that may have developed during volume production that could reduce effective operation of the item or result in item degradation. The CPT is conducted or supervised by an agent independent of the producer or by Government on-site quality assurance personnel, and may be conducted at procuring agency facilities, Government testing installations, or contractor facilities.

(3) Quality conformance (acceptance) inspections are examinations and verification tests normally prescribed in the technical data package for performance by the contractor and are subject to performance or witnessing by the on-site quality assurance representative on the items, lots of items, or services to be offered for acceptance under the contract or purchase order. These examinations and tests include, as necessary, in-process and final measurements or comparisons with technical quality characteristics required to verify that materiel meets all the terms of the contract and should be accepted by the Government.

(4) Tests in support of PDSS are DTs that are conducted during PDSS for software intensive materiel systems. They parallel those described for pre-FRP DR, but are usually abbreviated based on the number, magnitude, and complexity of the modifications or maintenance. Tests in support of PDSS are conducted to assure that software modifications meet requirements, do not impair existing functions or performance, can be employed by users, and are effective and suitable.

(5) A Service level test is the final preparation test prior to participating as a system under test in the joint interoperability test (see fig 6–1). The AMCOM SED serves as the Service level test agent for Army aviation, air, and missile defense systems. A Joint C4I interoperability certification test is conducted if major hardware and software modifications to the C4I system have been made that impact on previously established joint interface requirements. Re-certification test schemes must be developed and must be commensurate with the level of changes involved in both the C4I system and the systems with which it must interoperate. The CECOM SEC APTUC arranges, coordinates, and participates at all Joint interoperability testing with DISA, JITC, and coordinates the participation of all Army elements and systems. See JITC Plan 3006 JITP for testing TDL and USMTF systems is available at https://jitc.fhu.disa.mil/index.aspx. The AMCOM SED interfaces with the CECOM SEC to plan and schedule the Army aviation, air, and missile defense system participation in Joint C4I interoperability certification testing.

c. Post-production developmental testing. Post-production DT is conducted to measure the ability of materiel in the field, in storage, and following maintenance actions (reworked, repaired, renovated, rebuilt, or overhauled) to meet user's requirements (for example, conform to specified quality, reliability, safety, and operational performance standards).

(1) Surveillance/stockpile reliability tests include destructive or nondestructive tests of materiel in the field or in storage at field, depot, or extreme environmental sites. They are conducted to determine suitability of fielded or stored materiel for use, evaluate the effects of environments, measure deterioration, identify failure modes, and establish/predict service and storage life. For example, the PATRIOT program's Stockpile-to-Target Test Program. Surveillance test programs may be performed at the component-through-system level. System-level programs may include dedicated hardware allocated for this purpose, fielded materiel, or supplies in storage. "Libraries" of component parts to provide a baseline for subsequent surveillance test data comparisons may be established at contractor or Government facilities. Criteria for surveillance testing will be prescribed in the appropriate technical bulletins (TBs), technical manuals (TMs), storage serviceability standards, and surveillance test plans.

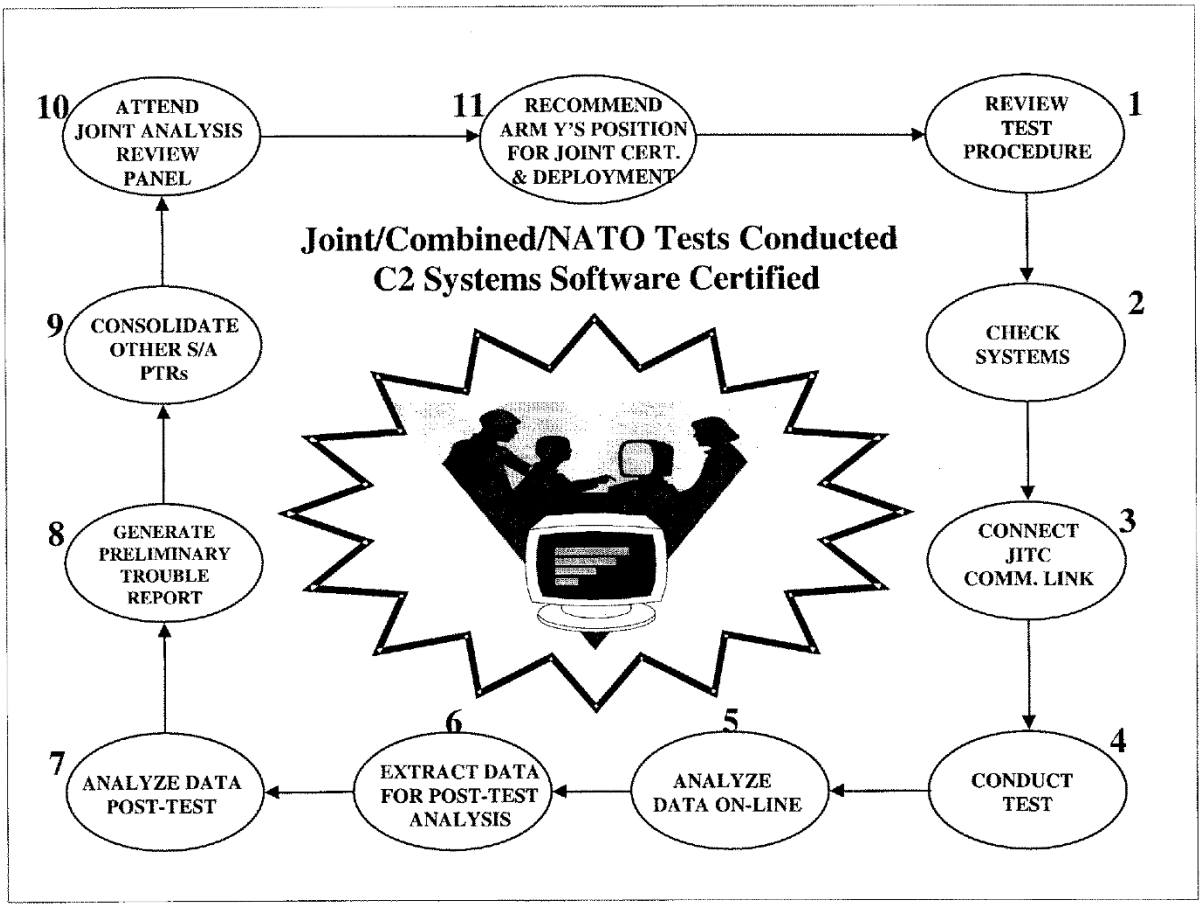


Figure 6–1. Joint/Combined/North Atlantic Treaty Organization interoperability testing cycle

(2) Reconditioning tests. Criteria for reconditioning tests will be incorporated in depot maintenance work requirements, modification work orders, TM, TB, and contracts. Reconditioning tests include the following categories:

(a) Pilot reconditioning tests are conducted to demonstrate the adequacy of the documented technical requirements, processes, facilities, equipment, and materials that will be used during volume reconditioning activities. The pilot model will be reconditioned in strict accordance with depot maintenance work requirements, modification work orders, TMs, TBs, and contracts. Pilot reconditioning testing relates to PVTs during production. Pilot reconditioning tests will be applied when depot maintenance work requirements, modification work orders, TMs, or TBs are used the first time or when major changes are made.

(b) Initial reconditioning tests are conducted to demonstrate the quality of the materiel when reconditioned under volume (rate) procedures and practices. These tests relate to FATs during production. Initial reconditioning tests will be conducted when an item is reconditioned for the first time by a Government or contractor facility, when changes in processes or facilities occur, or when there has been a significant break in reconditioning operations.

(c) Control tests are conducted on randomly selected items from volume reconditioning operations to verify that the process is still producing satisfactory materiel. Criteria should be the same as for initial reconditioning tests. These tests relate to CPTs during production.

(d) Acceptance tests are conducted on in-process materiel and when reconditioning activities are completed. An accept/reject decision by the procuring organization is based on acceptance testing.

(e) Baseline evaluation tests are conducted simultaneously on reconditioned and new production materiel of the same configuration to provide a comparison of performance and to determine the degree of reconditioning required. Baseline evaluation tests will be considered when the item is being reconditioned for the first time, when significant

modifications affecting performance are incorporated, or to provide data on which to base a decision regarding upgrading versus new procurement.

(3) Test criteria for post-production DT will be based on performance demonstrated during development and production. The number of items to be tested and the duration of tests will be based on sound engineering practices that consider schedules, costs, item complexity, known problem areas, statistical confidence, and other factors (for example, T&E WIPT proposed criteria and recommendations). Prior test data and analytically derived design data will be used when the test and sampling plan is developed. Existing test facilities will be used rather than building new Government or contractor facilities.

6–24. Requesting developmental test services

This paragraph provides procedures for requesting developmental test services from ATEC's DTC and SMDC's USAKA/RTS and HELSTF.

a. Program planning forecast. It is helpful to both the PMs/MATDEVs and the testing organizations to have early identification of future testing requirements. This permits the test agency to identify future requirements for test resources and provides a quantitative basis for test priorities and allocation of resources. It also supports requirements for facility development or upgrade, instrumentation development and acquisition, and test methodology studies, as well as justification for military construction plans to ensure scheduled tests can proceed without delay. When these future test requirements are identified, the MATDEV will be provided with a preliminary budget estimate and test schedule; however, this does not constitute a firm commitment by either party.

(1) Future testing requirements are generally those scheduled to occur beyond the next 180 days and cover the current fiscal year, the budget fiscal year, and the program objective memorandum (POM) years. When providing such forecasted test requirements, the MATDEV should provide as much of the information reflected in paragraph 6–33 as is available.

(2) Provision of future test requirements can be accomplished efficiently by an exchange of information through the T&E planning process. For example—

(a) As early in the acquisition cycle as possible, as T&E requirements are being considered during concept exploration and definition.

(b) During the preparation/review of the TEMP.

(c) As a result of negotiations at T&E WIPT meetings.

(d) During program reviews, test coordination meetings, and so forth.

b. Firm testing requirements.

(1) Firm test requests should be submitted as early as possible to allow the test agency to plan, coordinate, and schedule resources and ensure that required safety, security, and environmental concerns have been properly addressed prior to the test.

(2) The firm test request should include the information reflected at figure 6–2. Documentation required includes a safety assessment report, health hazard assessment report (HHAR), Security Classification Guide, environmental documentation (for example, record of environmental consideration, environmental impact statement (EIS), and environmental assessment) and SMMP (if required). If these documents are not available at the time the test request is submitted, the request should reflect a date as to when the documentation will be provided.

(3) Any other documentation or information that would enhance DTC's or SMDC's understanding of the test effort should be included.

c. Test requests. Test requests directed to the DTC may be submitted as follows:

(1) The most efficient way to request unclassified test services from DTC is through the Internet. Internet test requests are available anytime either through Army Knowledge Online or at https://www.atec.army.mil/. Upon submission of each request, the customer will receive a tracking identification number verifying receipt of the request and to be used for future reference.

(2) In writing to the Commander, DTC, ATTN: CSTE–DTC–TT–B, 314 Longs Corner Road, Aberdeen Proving Ground, MD 21005–5055. Requests may also be provided via email (ttb@dtc.army.mil), facsimile (DSN 298–9170), commercial ((410) 278–9170).

d. To request testing or additional information regarding SMDC's HELSTF. Contact the Director or Deputy Director at HELSTF Directorate, SMDC–TE–H, U.S. Army White Sands Missile Range, NM 88002–5148. The voice telephone number is DSN 349–5045/5074, commercial (505) 679–5045/5074.

e. To request testing or additional information regarding the SMDC facilities at RTS. Contact the Kwajalein Support Directorate, P.O. Box 1500, Huntsville, AL 35807–3801. The voice telephone number is DSN 645–3952, commercial (256) 955–3952; facsimile number is DSN 645–1880.

6–25. Developmental test readiness review

The DTRR is chaired by either the MATDEV or developmental tester and is conducted to determine if the developmental item is ready for DT. As a minimum, the DTRR is conducted prior to PQT for materiel systems or SQT for non-tactical C4/IT systems. While not as rigid, the DTRR schedule could parallel that recommended for OTRRs. (See para 6–45*b*.)

The following information is required for Firm Test Requests (and can be tailored to reflect individual requirements):

Test item nomenclature (model number, lot number, short title, and acronym). Reflect the individual project title as identified in the Army Research, Development, and Acquisition Plan or other budgetary documents.
Item description. Identify unique characteristics that might require special test and analysis requirements. Include existing or planned systems with which the item will interface. State if a materiel change management program (citing MC number) or a Foreign Military Sales (cite FMS case number and country).
System life cycle phase. Identify the phase or the milestone decision review being supported by the test. State the ACAT designation and if the program is on the OSD T&E Oversight List, specifically for the Live Fire.
Funding. Type of funds to be provided (for example, R&D, procurement, OMA) and associated funding code (program element / task for R&D and OMA, standard study number for procurement).
References. Identify DTC project number if previously forecast and reference ORD, TEMP, SEP/EDP, and military specifications.
Description of test. Provide the test type, a brief description of the test, and test data required to answer preliminary concerns of the MATDEV. Include the appropriate test type as defined in DA Pam 73-1, paragraph 6-23. (NOTE: The requirement document can be provided to address these requirements.) Any additional pertinent documentation (for example, other test plans, specifications, MIL-STDs) that would assist in development of the scope of work should be referenced.
Test schedule. Include quantity of test items and delivery date (month and year). Provide any milestones requiring special consideration, such as required completion of testing, SER due date, and so forth.
Report requirements. Indicate type of report required (that is, test record, abbreviated report, or formal report) and distribution requirements. Include firing and Test Incident Report (TIR) requirements.
Administrative and technical points of contact. Name, organization, office symbol, telephone number, and email address.
Safety considerations. Address any safety problems and considerations concerning the test item. Provide a copy of the Safety Assessment Report (SAR). NOTE: Policy dictates that government developmental testing will not begin until a SAR has been received from the test sponsor and reviewed and accepted by the government organization performing the test (AR 385-16).
Environmental considerations. Cite any environmental considerations that might impact on the accomplishment of the requested effort and provide the appropriate documentation in accordance with the National Environmental Policy Act (NEPA) and AR 200-2 (for example, Record of Environmental Consideration, Record of Environmental Impact Statement, or Environmental Assessment).
Security considerations. Address applicable provisions of the security classification guide or security checklist and any applicable OPSEC requirements.
Requirements for standard/non-standard ammunition. State the requirements for ammunition.
Disposition instructions. Provide guidance on return or disposal of test items.

Figure 6–2. Firm developmental test request

6–26. Developmental test readiness review working group

The DTRR working group, whose members include the core T&E WIPT members plus others as deemed appropriate, reviews all pre-test start activities and requirements that may impact the execution of the test as planned by the T&E WIPT. The objective of the review is to determine what actions are required to ensure resources, training, and test hardware will be in place to support the successful conduct of the test, and to ensure that T&E planning, documentation, design maturity/configuration, and data systems have been adequately addressed.

a. The DTRR working group is typically composed of the following representatives—

(1) MATDEV.
(2) MATDEV's Safety Office.
(3) MATDEV's ILS Office.
(4) MANPRINT representative.
(5) MATDEV's Product Assurance and/or Testing Office.
(6) CBTDEV or FP.
(7) Developmental tester.
(8) Operational tester.
(9) System evaluator.
(10) Logistician.
(11) Trainer.

b. Others who may be requested to participate are—

(1) Foreign intelligence officer.
(2) DCS, G–2—threat integration staff officer (TISO).
(3) Transportability analyst.
(4) OSD action officers.

c. The DTRR working group should be formed for all programs on the OSD T&E Oversight List. For programs not on the OSD T&E Oversight List, establishment of a working group is at the discretion of the MATDEV. In cases where a full DTRR is not conducted, the MATDEV should conduct a preliminary DTRR to assure that the item or system can successfully complete the planned testing.

6–27. Developmental test readiness review procedures

a. The chairperson, after initial coordination with the membership, notifies and provides each member a DTRR package ensuring that all considerations (see fig 6–3) have been addressed. Figure 6–4 depicts a typical DTRR agenda. Notification of the time and location of the review plus the DTRR package should be provided at least 2 weeks before the review to allow members to determine the proper level of representation by their organization and to effect preliminary internal coordination. Member agencies will determine the extent of their representation. Since all representatives may not attend each review, the chairperson may indicate recommended attendance.

b. As applicable, the DTRR package consists of the following documentation:

(1) A T&E WIPT coordinated TEMP.
(2) SEP and, if required, developmental test EDPs.
(3) Developmental tests and DTPs.
(4) Safety Assessment Report.
(5) Applicable environmental documentation.
(6) Current test hardware configuration.
(7) RAM assessment to include statement of best estimate for the current value of system reliability and likelihood of meeting RAM test objectives.
(8) RAM failure definition/scoring criteria.
(9) A statement of the status of the SSP.
(10) A statement of the status of new equipment training (NET).
(11) A statement of the status of MANPRINT.
(12) A statement of the status of instrumentation and data collection and reduction facilities.
(13) An ILSMT-approved integrated logistic support plan.
(14) An airworthiness statement.
(15) A statement on the status of software.
(16) Safety release.
(17) DT threat TSP.

The following factors should be taken into consideration when preparing a DTRR package for a PQT for a program on the OSD T&E Oversight List. This list should be modified for programs not on the OSD T&E Oversight List, as required.

1. General - Compare the requirements document against test results to date. There must be a reasonable assurance (confidence) that the system to be tested can satisfactorily pass developmental test or equivalent independent government tests.

a. Previous data sources should indicate that system requirements could be met. (Consider quantities tested, what tests were conducted, and results.)
b. All system requirements must be addressed.
c. All critical / major problems identified in TIRs from previous testing should have been corrected and verified. (List and summarize corrective actions.)

2. Safety

a. A Safety Assessment Report (SAR) (AR 385-16) and a Health Hazard Assessment (HHA) (AR 40-10) must be submitted to the testing agency.
b. A System Software Working Group (SSWG) should have been formed.
c. System safety limitations (operational limitations for test personnel) should be identified, either inside or outside the required performance envelope. Corrective action should have been taken or be planned.
d. Critical defects found during manufacture/loading/inspection of the items should be identified.
e. A SSMP should be established.
f. The contractor should have established a System Safety Program Plan (SSPP).
g. All residual risks should have been identified and managed per AR 385-10 and AR 385-16.
h. Review of the USASC's Independent Safety Assessment prepared at each MDR.

3. Reliability, Availability, and Maintainability

a. Reliability and maintainability predictions should be included.
b. Reliability growth goals should have been met.
c. Critical components identified and component testing conducted.
d. An independent RAM assessment conducted.
e. Failure definition/scoring criteria established.

4. Configuration Management

a. A preliminary product baseline technical data package should have been established.
b. A configuration management plan should be in place, which includes provisions for Government approval of engineering change proposals and waivers/deviations.
c. A Configuration Control Board should have been established.

5. Electromagnetic Environmental Effects (E3)

a. Hardware conformance to the baseline evaluated. A physical configuration audit should have been conducted. Consideration should be given to how many items and the results.
b. Test item configuration should be compared with items previously tested.
c. Any unresolved risks should be identified.
d. Human factors evaluations should have been conducted.
e. Unique (nonstandard, new, or proprietary) manufacturing and/or functional processes identified.

6. Software

a. Configuration items related to software should have been identified and controlled.
b. All software test plans/procedures/test results should have been reviewed/approved by the Government.

Figure 6–3. Considerations in preparation for the developmental test readiness review

c. All functional requirements should be clearly identified.
d. Confidence that software functions will execute properly (walk-through, design specs, program performance specs, interface specs, resource allocations).
e. A clear understanding should exist of what software functions will be tested by the developmental and operational testers.
f. If applicable, the Computer Resource Management Plan should be current.
g. Plans should have been formulated to deliver all software documentation prior to DT/OT.

7. Test Documentation

a. The detailed test plan should address all critical technical parameters and be approved.
b. If required, the Human Use Committee should have approved the detailed test plan.
c. Airworthiness and Safety Releases should be provided and all recommendations complied with. [Rationale: Issuance of a Safety Release or Airworthiness Statement may require changes in system design. Workarounds and special operational procedures, training, to be implemented before the system is safe for soldiers' use and ready for test.]
d. Required environmental documents should have been received.
e. Instrumentation plans should be prepared and approved.
f. If required, an Outline Test Plan should have been prepared and submitted.

8. Integrated Logistics Support

a. Supportability.
(1) SSP Component List (SSPCL) prepared and coordinated with all concerned agencies. (See AR 700-127.)
(2) All items on the SSPCL available at each test site prior to test, or a waiver approved.
(3) All manuals (including drafts) available, including those for support equipment, associated equipment software, and TMDE.
(4) A logistics demonstration conducted.
(5) Testing for supportability included in the TEMP, OTP, SEP, EDP, and DTP.
(6) Field support equipment should be available for test.
b. Transportability Testing. System transportability needs should be identified (including such requirements as lifting and tie down provision strength, helicopter lift, Air Force aircraft loading, air drop, and rail impact).

9. MANPRINT

a. MANPRINT analyses conducted.
b. System MANPRINT management plan prepared.
c. Human factors engineering analysis accomplished.
d. Training.
(1) NET for test personnel accomplished prior to the start of DT.
(2) NET TSP prepared. (See AR 73-1.)
(3) Training devices, aids, and/or equipment needed by NET personnel available.
e. Soldier survivability should be addressed.

10. Test Resources

a. Required agencies should be funded for the test.
b. Unique facilities/equipment instrumentation required should be available at the test site(s).
c. Sufficient test articles must be available.
d. Sufficient targets and threat simulators should be available.
e. Required targets and threat simulators validated and accredited for this test.

11. Security Considerations

Status of DITSCAP accreditation.

Figure 6–3. Considerations in preparation for the developmental test readiness review—Continued

1. **Purpose**

2. **Program Sponsor Issues** (Program Sponsor)
   a. System Equipment Status.
   b. Results of previous testing and/or data sources.
   c. Safety Issues; Safety Release and Safety Assessment Report approved.
   d. System Delivery Schedules (Milestone).
   e. Contractors Support (if applicable).
   f. Logistics Support Plan.
   g. Test Instrumentation.
   h. Other Special Topics.

3. **Reliability, Availability, and Maintainability**
   a. Status of Independent RAM assessment.
   b. Failure definition/scoring criteria established/approved.

4. **Software**
   a. Configuration Management Plan in place.
   b. Preliminary product baseline technical data package established.

5. **Electromagnetic Environmental Effects (E3)**
   a. E3 criteria established and/or approved.

6. **Test Documentation (Developmental Tester)**
   a. TEMP coordinated/approved.
   b. System Evaluation Plan/Detailed Test Plan, and Test Operations Procedures (TOPs), (approval). Overview of the test design to include issues as appropriate and status of SEP development.
   c. Resources. Status of support required/received, unique facilities, special instrumentation available at the test site(s).
   d. Test Schedule
   e. Participation/Other Agencies (if applicable)
   f. Data Collection Reduction and Processing Plan
   g. Human factors and the status of the MANPRINT statement.
   h. Human Use Committee approval of the DTP, if required.
   i. Airworthiness statement, if required.
   j. Outline Test Plan approved, if required.
   k. Sufficient test articles.
   l. DT Threat Test Support Package available.
   m. Sufficient targets and/or threat simulators available.
   n. Targets and simulators accredited for this test
   o. Other Special Topics.

7. **Integrated Logistics Support**
   a. System Support Package completed.
   b. SSP Component List (SSPL) prepared and coordinated and SSPL items available.
   c. System transportability requirements and testing, identified.

8. **Discussion** (All)

9. **Decision** (Chairman)

Figure 6–4. Sample developmental test readiness review agenda

(18) Threat accreditation report.
(19) Status of transportability statement.
(20) Developmental test readiness statement (DTRS) (for PQT or SQT only).

Note. See appendix U for the formats associated with these documents.

c. After coordination with all participants, the DTRR working group will be convened at the call of the chairperson.

d. The DTRR working group makes recommendations on all issues regarding T&E planning. Each representative has the responsibility to advise participating members in test matters considered to be of mutual concern.

e. In the event of disagreement among the members, issues are presented to the chairperson for resolution through normal command/staff channels.

f. The chairperson provides minutes of the DTRR that include a DTRS. This statement verifies that the system is ready for DT, or if there are action items identified during the review that must be satisfied before test can begin, the minutes will identify such actions. The MATDEV will ensure that all requirements are satisfied before the test begins. The minutes, including all recommendations, issues, and required actions are distributed to each DTRR participant 10 working days after the DTRR.

6–28. Developmental test event design plan

Guided by the SEP, the EDP states the data required and any special test analyses procedures for the system evaluation. The EDP is prepared by the system evaluator and coordinated with the T&E WIPT. It provides explicit instructions for the conduct of developmental tests and subtests. It is coordinated with the MATDEV and approved by the test organization's parent command. For a system contractor-conducted DT, the MATDEV approves the EDP.

a. The EDP addresses all DT parameters and reflects all program constraints (such as dollars, test quantities, schedules, and issues). As a minimum, the EDP should address the test objectives, test concept/methodology, system description (to include component-level or system-level), test personnel requirements, test criteria, test schedule, and required coordination. In addition, the EDP must spell out the form in which the data are needed and the accuracy with which they must be measured.

b. Each subtest should be addressed separately, stating the criteria to be addressed by the subtest, the data to be obtained during the test, the procedures to be used, and data presentation (that is, statistical methods and confidence levels). The procedures should be described in sufficient detail to reflect what will occur during the test. Performance standards and test operating procedures should be used, if possible, and referenced in the EDP. The EDP for LFT&E is coordinated with the members of the LFT&E WIPT.

c. The EDP will also contain the appropriate reliability test strategy, sample sizes, design of tests/experiments, minimum test requirements to measure performance specified, requirements for data and the process by which the data will be verified, and identify tests in order of priority to ensure that the more critical data are generated early.

d. The live fire test EDP provides further detail on the critical issues developed in the LFT&E TEMP strategy (see app J). The SEP provides the crosswalk between the live fire critical issues and the data sources. The LFT EDPs define the data requirements and data sampling plan and analysis techniques are specified to ensure the logic of the evaluation is understandable. As a minimum, the LFT&E EDP should contain the following—

(1) A cover page providing the name of the system, the activity/agency responsible for preparation of the plan, date, classification, and applicable distribution statement.

(2) A coordination sheet containing the signatures of the approval authorities.

(3) Administrative information: name, organization, telephone, and email addresses of key LFT&E personnel.

(4) Description of threat weapons or targets that the system is expected to encounter during the operational life of the system, and the key characteristics of these threats/targets which affect system vulnerability/lethality; a reference to the specific threat definition document/authority; discussion of the rationale and criteria used to select the specific threats/targets and the basis used to determine the number of threats/targets to be tested and evaluated in LFT&E.

(5) If actual threats/targets are not available, then the plan must describe the threat/target surrogate to be used in lieu of the actual threat/target, and the rationale for its selection.

(6) A statement of the test objectives in sufficient detail to demonstrate that the evaluation procedures are appropriate and adequate.

(7) A description of the shot selection process. Describe the process to be used to establish the test conditions for randomly selected shots, including any rules (exclusion rules) used to determine whether a randomly generated shot may be excluded from testing. For engineering shots (for example, shots selected to examine specific vulnerability/lethality issues), describe the issue and the associated rationale for selecting the specific conditions for these shots. List the specific impact conditions and impact points for each shot, and whether it is a random or engineering shot.

(8) A description of data requirements for each LFT test.

(9) A description of the analysis/evaluation plan for the live fire program from the SEP. The analysis/evaluation plan must be consistent with the test design and the data collected. Indicate any statistical test designs used for direct comparisons or for assessing any pass/fail criteria.

6–29. Developmental test incidents and related reports

Timely reporting of test results is essential and is accomplished through TIRs as well as the formal test reporting procedures. Test incident data are prepared by the test organization (Government or contractor) to provide the results of any incident occurring during testing that may assist in explaining the test data. In response, as a minimum, the MATDEV prepares corrective action data for all critical or major TIRs. Corrective action data reflect the developer's analysis of the problem and the status or description of the corrective action. All data are put into the ATIRS to enhance the CE of the program. ATIRS is administered by the ATC of ATEC's DTC at Aberdeen Proving Ground, Maryland. Details of test incidents and related reporting are contained in appendix V.

6–30. Developmental test detailed test plan

The DT DTP is prepared by the developmental test activity. It is based on the SEP and EDP, if available, and provides explicit instructions for the conduct of the DT.

a. Coordination. The DTP is coordinated with the system evaluator and may be coordinated with the T&E WIPT to ensure that the test data meet the requirements of the TEMP. The DTP is approved by the test activity's parent command; if a contractor-conducted test, the DTP is coordinated with the system evaluator and then approved by the MATDEV.

b. Content. The DTP governs test control, data collection, data analysis, and the necessary administrative aspects of the test program. As a minimum, the DTP should address the objectives, test concept, system description, test personnel requirements, test criteria, test schedule, and required coordination. Each subtest is addressed separately. Performance standards and test operating procedures may be used and referenced in the DTP.

c. Live fire detailed test plan. For specific guidance on the LF DTP, see appendix S.

6–31. Developmental test report

For T&E WIPT-coordinated DT, the test report is provided by the test agency (either contractor or Government) to T&E WIPT members and the DR body at the conclusion of the test. For extended test phases, an interim test report may be submitted for interim reviews. Test results must be comprehensive and complete before presentation to the MDA. DT performed to support efforts not involving the T&E WIPT will report test results to the test sponsor according to the test sponsor's requirements.

a. As a minimum, final draft test reports, authenticated by the test agency, are required prior to DRs. This is in consonance with policy regarding other documentation supporting the acquisition of a weapon system. The T&E WIPT should conduct a review 30 days prior to the DR to review the adequacy of past tests, test results and evaluations, planning for future testing, and the modification of test strategy to accommodate the evolving acquisition strategy. Issues not resolved in this forum will be elevated to the IIPT, OIPT, and, lastly, the DUSA (OR). The test activities that conducted the developmental tests prepare, approve, and publish the test reports. Test reports for contractor-conducted developmental tests are approved by the MATDEV.

b. The format of the formal test report parallels that of the DT DTP. An executive digest provides a summary of the significant findings, the test objectives and concept, and a description of the test item. Subtest results include, in addition to the objectives, criterion, test procedures, test findings, and a technical analysis of the data that relate to each subtest criteria addressed. Appendices include the test program criteria (from the DT DTP), and if required, lengthy test data presented as tables, charts, and illustrations. The formal test report may include a preliminary determination of deficiencies, shortcomings, and suggested improvements.

c. For live fire testing of ACAT I programs and other live fire OSD T&E oversight programs, the developmental tester must submit the developmental test reports to DOT&E through the DUSA (OR). If the test report is not available, an interim report will be submitted. Guidance for preparation of the final test reports for FUSL live fire tests is provided in appendix S.

6–32. Testing for climatic suitability and effectiveness

MATDEVs plan for realistic testing in accordance with system life cycle environmental profiles, as presented in MIL–STD–810. Systems will be tested for their ability to remain safe, effective, suitable, and reliable in those environments where they will be operated, handled, transported, and stored. Natural field environments, representing all of the various climatic design types described in AR 70–38 are available at ATEC test centers.

a. Testing in climatic chambers. Prior to testing in natural environments, MATDEVs plan for simulated environmental testing in climatic chambers unless impractical. Results of climatic chamber tests may be used to determine if a system will not satisfy its performance requirements. Chamber tests may also be valuable in assessing the risk associated with not conducting tests in the natural environment. Causes for failures in simulated environments must be resolved before the system is subjected to natural environment testing. Chamber tests and simulations play a significant role in the beginning of the development cycle, but must be integrated with testing conducted in real world, natural environments. Test results from climatic chambers cannot be interpreted as a total substitute for tests conducted in the natural environment, because they do not provide the synergisms associated with the natural environment.

b. Testing in the natural environment. MATDEVs will test, as a minimum, in the basic design types (see para 6–33) to ensure the system will be subjected to the synergistic effects those natural environments provide. The effects of many environmental variables can be seen at once and MPs can be followed. Data derived from these tests will be used to evaluate suitability and effectiveness. Potentially dangerous systems (for example, ammunition) will be tested to all climatic design values regardless of their requirement to operate in those climates. Therefore, a level of risk exists that a system may meet all of its operational requirements, but not be suitable for fielding. See appendix W for details on survivability testing.

6–33. Basic climatic design type

a. Per AR 70–38, the Army recognizes four climatic design types: hot, basic, cold, and severe cold. Generally, Army systems must be designed in accordance with the operational requirements. Thus, systems operate in and are designed, as a minimum, for the basic climatic design type. Some systems may require testing in the more severe climatic design types if their life cycle environmental profiles (see MIL–STD–810) identifies potential exposure to them. The basic climatic design type has four daily weather cycles as depicted in table 6–1.

Table 6–1
Basic climatic design type

Daily cycle	Ambient temperature (degrees F)	Solar radiation (BTU/FT2 per hr)	Relative humidity (%)	Storage temperature (degrees F)
Basic hot	86–110	0–355	14–44	86–145
Basic cold	-5 to -25	Negligible	Toward Saturation	-13 to -28
Tropic (constant high humidity)	75 (constant)	Negligible	95–100	80 (constant)
Temperate (variable high humidity)	78–95	0–307	74–100	86–145

b. Other environment factors (both natural and induced) must be taken into consideration during testing. The natural environment factors are listed at table 6–2.

Table 6–2
Environmental factors

Natural factors	Induced factors
Terrain	Atmospheric pollutants/smoke
Animal life	Vibration
Humidity	Acceleration
Solar radiation	Blast pressure
Ozone	CB contamination
Wind	Laser emissions
Salt, salt fog, and salt water	Sand and dust
Microbiological organisms/mold	Shock
Vegetation	Acoustics/noise

Table 6–2
Environmental factors—Continued

Temperature	Electromagnetic radiation
Pressure	Nuclear radiation
Rain	RF emissions
Fog and whiteout	Acidic atmosphere
Solid precipitation	
Microbiological organisms	
Lightning and static electricity	

(1) While it is necessary to recognize the importance of individual natural environment factors, it is equally, if not more important to recognize the combined effects of related environment factors. These factors may interact to produce effects on materiel different or more severe than the sum of the effects caused by individual factors acting independently. The relationship among the various individual environment factors and the four weather cycles can be found in AR 70–38.

(2) The prime example of combined factors that are often forgotten in the design of equipment is the effect of high temperatures and solar radiation. AR 70–38 indicates that the maximum high temperature is 110 °F, and many designers use this as the basis for their designs. What may be forgotten is an item that is painted camouflage colors may absorb as much as 360 BTU of solar radiation per square foot of exposed surface/per hour, which will significantly raise both internal and external temperatures.

(3) The natural environment factors experienced by equipment in a given time or place are related to the protection provided. An example of this would be the difference in materiel exposed to ambient climatic factors resulting from open storage versus environmentally controlled storage.

c. Induced environment factors are mixed in their relationship to natural factors as some are strongly related in their effects on materiel and some are virtually independent. See table 6–2.

(1) Since induced factors are generally independent, they can be tested in laboratory or chamber conditions using approved procedures such as those described in MIL–STD–810 and under environment conditions described in AR 70–38. For example, the effect of vibration can be quickly and accurately tested under controlled conditions instead of having to transport and handle the item for long periods of time.

(2) The opposite is true for natural environment factors. Chamber tests can only assist in the development of an item and are not a substitute for the real world environment because of the interaction of the natural factors.

Section III

Operational Testing

6–34. Overview of operational testing

The primary objective of OT in support of the acquisition process is the verification of operational goals and objectives, generally defined by the COIC. The structuring and execution of an effective OT program is absolutely essential to the acquisition and fielding of Army systems that are operationally effective, suitable, and survivable while meeting the user's requirements. There are many elements integral to a successful OT program. This section provides procedural guidance in the following areas:

a. Planning, executing, and reporting OT for material and C4I/IT and space systems.

b. Addressing RAM, ILS, MANPRINT, threat, survivability, compatibility, interoperability, and M&S in support of OT.

6–35. Operational test objectives in support of the materiel and tactical C4I/IT systems acquisition process

OT is conducted in a realistic environment on all systems with typical users (that is, Soldiers and civilians) in as realistic an operational environment as possible. OT uses personnel (that is, operators, maintainers, and administrators) with the same skills and training as those who will operate, maintain, and support the system when it is deployed. A realistic operational environment includes tactical operations conducted in accordance with the system's wartime OMS/MP, which specifies the number, type, and frequency of combat operations during a period of time. The

scenarios used in OT should use the TTPs, doctrine, logistics, training, and maintenance support concepts planned for use when the system is fielded.

a. The OT threat represents threat systems capabilities and threat tactics and doctrine postulated at post-fielding. The environment for these operations may include—

(1) The employment of opposing forces.
(2) Electronic and other enemy countermeasures.
(3) Simulated NBC warfare.
(4) Smoke and other forms of battlefield obscuration.
(5) Terrain and weather.

b. OT can provide data not obtainable through other sources. It is applicable for all development systems, commercial items, NDI, and product improvements, unless waived (see AR 73–1) or not required by the TEMP or the approved acquisition strategy.

c. OT may provide data useful for the development or refinement of the JMEM that will accompany the system at IOC, and may provide an opportunity to evaluate a draft JMEM if one has been developed prior to OT/IOT. In any event, consideration should be given to JMEM requirements during OT planning and execution.

6–36. Origin of operational test requirements

OT requirements result from the OSD JT&E Program, multi-Service and Army TEMPs, CEPs, and MATDEVs and CBTDEVs with special testing needs (customer tests). OT planning, documentation, resource identification, and execution are conducted through a variety of means. Committees and working groups (such as OSD JT&E and Joint Feasibility Study, T&E WIPTs, Army TSARCs, ATEC OTRRs, and SMDC's T&E Center and test directorates) support the overall process and aid in OT event coordination.

6–37. Operational test types

a. An EUT is a generic term encompassing all system tests employing representative user troops during concept and technology development or early in system development and demonstration. The purpose of EUT is to test materiel concept, support planning for training and logistics, identify interoperability problems, and identify future testing requirements. EUT provides data for system evaluation supporting the MS B or MS C decision. FDT/E or CEP may comprise all or part of EUT. An EUT is conducted with RDT&E funds. An EUT uses procedures described for IOT, modified as necessary by maturity and availability of test systems and support packages. EUT seeks answers to known issues that must be addressed in the SER.

b. A LUT is any type of RDT&E funded OT, other than IOT, normally conducted during systems acquisition in support of the LRIP decision. LUT addresses a limited number of evaluation issues and is used to accomplish the following objectives—

(1) Testing necessary to supplement DT before a decision to purchase long-lead items or at MS C.
(2) Testing necessary to verify a fix to a problem discovered in IOT that must be verified prior to the production decision (for example, problem is of such importance that verification of fix cannot be deferred to FOT).
(3) As needed to support NDI or modifications that may not require a dedicated phase of IOT before a production decision.
(4) A LUT will not be used to circumvent requirements for IOT before a production approval decision as prescribed by statute, DoDDs, and AR 73–1.
(5) A LUT will not be used to piece-meal IOT through a series of limited objective tests.
(6) A LUT can be conducted post-IOT to address recurring modifications to software.

c. An IOT is an operational test that is conducted to support the FRP DR. IOT for developmental systems includes all system components, such as hardware, associated support packages, ground support, computer software, training, TMDE, and all systems with which the system under test must operate. Waiver requests for IOT must be supported by plans and schedules for obtaining relevant data from other sources. IOT is characterized by—

(1) Use of production-representative systems.
(2) Organizational units, tables of organization and equipment units, provisional units, or elements typical of those that will employ and support the system and have received Soldier and leader training planned for the system when initially deployed.
(3) Employment under realistic simulated combat conditions equivalent to those expected during the IOC timeframe and against the threat postulated for the system's deployment. The threat capabilities are normally representative of those projected for IOC plus 10 years. The T&E WIPT will determine the appropriate post-IOC timeframe for which the threat needs to be represented in the IOT.

(4) Traditional weapon system OT requires the entire system to successfully complete OT of production representative items before fielding. The strategy allows fielding of parts of software intensive systems, once successful OT of a representative sample has been accomplished.

d. A FOT consists of the following—

(1) Conducted after a system enters FRP. FOT is conducted to ensure that production items remain operationally effective, suitable and survivable, validate corrections to identified operational deficiencies, verify corrections of training and logistical deficiencies, and resolve issues remaining after the FRP DR. FOT is conducted on production items using the IOC or other applicable units.

(2) System evaluator should minimize the need for FOT by making maximum use of other data sources. As much as possible, FOT uses current and complete system support packages; organizational structures; employment doctrine; support requirements; threat; command, control, communications, and intelligence (C3I); tactics; training; and interfaces with other systems.

(3) System evaluator tailors the extent of the FOT to answer the issues resulting from the IOT or new issues from the acquisition community. The FOT may be conducted either in the same manner and depth as an IOT or it may be conducted for limited objectives in the same manner as a LUT or a FDT/E.

e. A customer test (CT) is a test conducted by a test organization for a requesting agency external to the test organization. The requesting agency coordinates support requirements and provides funds and guidance for the test. It is not directly responsive to Army program objectives and is not scheduled or approved by the TSARC.

6–38. Operational testing of non-tactical C4/IT and space systems

a. OT of all non-tactical C4/IT and space systems will be conducted in a realistic operational environment, using troops or assigned civilians from representative units or organizations, and incorporating the approved threat.

b. A supplemental site test may be necessary for those systems, which execute in multi-hardware and -operating system environments. The supplemental site test supplements the IOT and user acceptance test (UAT).

c. IOT in support of a FRP DR is called an IOT. Between FRP and system retirement, testing is called PDSS for C4I/IT systems.

d. A UAT may be conducted by the FP or CBTDEV. It is limited in scope relative to a FOT and serves primarily to verify the functionality of the changes to the non-tactical C4/IT system in the user environment.

6–39. Operational test planning

When a test activity is assigned responsibility for execution, OT planning begins. Planning includes development of the overall test design and documenting the actions required to provide the data to address system evaluation requirements or to answer customer requirements. These events may be in support of an Army acquisition program, concept experimentation, FDT/E, ACTD or other events such as CTs.

6–40. Operational test planning process

a. The OT planning process generally consists of the performance of a variety of functional area requirements that may vary significantly dependent upon the type of test. Tests and experiments will normally require most, if not all, of the functions to be performed. Other events, such as market investigations or M&S activities may require performance of only a subset of the areas. The overall planning process follows a logical sequence of functions:

(1) Identifying event requirements from appropriate sources;

(2) Developing the design for the event;

(3) Identifying event control and scenario and/or test schedules, as well as data management, training, resources, instrumentation, administrative and logistical, and other appropriate requirements for the event.

b. Performance of these functions generally falls into phases consisting of preliminary analysis and planning, test design, and detailed test planning procedures. The results of preliminary analysis and planning and test/event design are documented in an event planning document, either an EDP, Test Plan (TP), or DTP depending on the type of event and test activity performing the event. The results of detailed test/event planning procedures are documented in the executing command's event execution plan that contains the details required for day-to-day event execution.

c. The core element of event/test planning is the development of the event design.

(1) The event design process identifies the independent, dependent, and uncontrolled variables; the treatments of the independent variables to produce the desired effect on the dependent variables to generate required test data under the appropriate conditions; and required numbers of executions to provide desired level of confidence in test results. An additional consideration is the overall event methodology for any comparison purpose. This methodology may be comparison of a new system to a baseline or to specific standards, performance of an organization with the system to an organization without the system, or just to obtain specific data pertaining to elements of system design or

performance requirements. The conditions under which the event is to be conducted also greatly impact event design. Simulation of operational combat conditions and tactical operations may require greater degrees of event design than for other types of events. The degree of detail of event design may vary significantly dependent on the type of event, number of independent variables, and event environment requirements.

(2) Certain requirements for event design may be met by predetermined standard operating procedures (SOPs) that do not change significantly from system to system. Other event design requirements may necessitate the creation of a complex event design involving player forces, real time casualty assessment, and considerable operational environment simulation from event source material. These requirements, singly or in combination, occur for many OT events. Regardless of the methodology and degree of depth required for the design, core event design forms the basis for all other event planning requirements.

(3) Event designs are clearly and comprehensively described in the event planning document. The event design should provide the overall methodology and design for conduct of the event. Essential information should be shown in a format that most clearly shows what is to be performed and how it will be performed. Overviews of phases, expected or required sample sizes, and organization of trials in accordance with the various combinations of independent variables should be shown in tabular or graphic form that provide for best understanding of the information. Descriptions of other key information should be structured to "paint the picture" for the decision maker and other readers. Clear understanding of the design is critical for all personnel and will ultimately lead to a better-executed event.

d. In general, the event planning process is conducted as depicted in figure 6–5. While a number of sources are shown as inputs to the overall process, many other potential sources exist for specific types of events or for unique event requirements. Event planners must consider all identified sources in determining overall requirements to ensure the event results in usable and creditable information for the overall purpose. The results of the planning are documented in the EDP, DTP, or TP. If required, an event execution plan is also used for documentation of day-to-day actions. Resource requirements for OT (and DT requiring Soldiers) are normally documented in the OTP. (See AR 73–1.) Requirements for ATEC resources for events other than OT (or DT) are documented in the ATEC Decision Support System (ADSS) (https://adss.atec.army.mil/). Requirements for SMDC T&E resources are coordinated through the SMDC's T&E Center, Huntsville, AL, DSN: 645–2742 or 2736, commercial (256) 955–2742 or 2736.

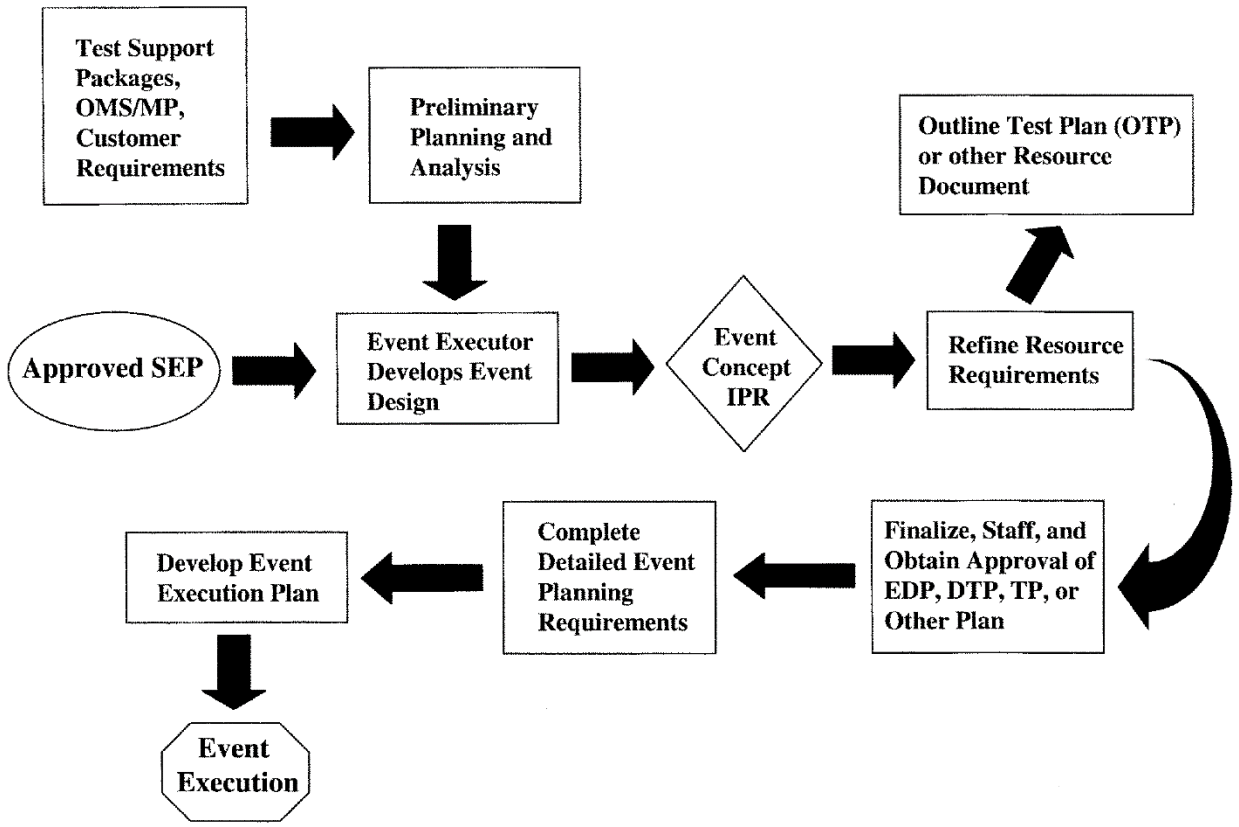


Figure 6–5. Event planning process (repeated for each event)

6–41. Operational test event planning documentation

a. An EDP is prepared to document planning actions for an event or combination of events identified in the SEP as needed. The EDP documents the test design, supporting methodology, and analytic details required for the specific event when the information is not contained in the SEP. All OTs and combined DT/OTs will have an EDP. Integrated DT/OT may prepare a separate plan or combine plans into a single document.

b. As appropriate for the level of planning, an event execution plan (generic term) containing the necessary details for day-to-day execution of the event will be prepared. The EDP, when required, along with the event execution plan, will document planning for assigned events in accordance with the executing command's policies. An event execution plan may be ATEC's OTC EDP, DTC's DTP, or DTC's test operating procedures or International Test Operations Procedures (ITOPs). The test command will tailor the procedures and documents consistent with the ACAT of the system, the SEP or customer requirements.

c. Executing commands for OT events (and DT events requiring user test personnel) will prepare an OTP documenting event resource requirements. The OTP will be submitted through the Army TSARC process for resource approval and required tasking actions (see AR 73–1). Commands may use the Resume Sheet (RS) for documentation of resources that do not require TSARC review. The OTP will be fully coordinated with the T&E WIPT to advise resource providers of the estimated T&E support requirements.

d. The T&E activity team develops EDPs in coordination with the T&E WIPT for assigned acquisition program events. The operational test organization leads the development of EDPs for operational tests. The assigned executing command solely develops plans for all non-acquisition program related events, such as a CT, CEP, or non-system related FDT/E.

e. The EDP for events that are not directly in support of an acquisition program are approved by the executing command.

f. Event execution plans do not require formal staffing and approval outside of the executing command. For acquisition program events, if requested, the OT execution plan will be made available to T&E WIPT members for reference and information during the event planning to assist in understanding of overall event requirements.

6–42. Operational events

Operational events can generally be defined as those OT and experimentation events conducted to support Army acquisition program requirements and other events; whether test, experimentation, or exploratory; that are conducted in simulated operational or combat environments with typical user troops and, as appropriate, representative material. The key difference of an operational event from other types of events is the employment of typical users operating the system under test in the environment under which the system is expected to operate when deployed.

a. The T&E activity teams may provide input for or participate directly in the planning for operational events for acquisition programs. However, the majority of the planning requirements for these events and for non-acquisition related operational events are conducted by the T&E activity test directorate.

b. Operational event planning will require actions in many areas due to the nature of simulating an operational environment and conditions. Some of these actions will address how to simulate the expected operational environment; integration of the system within a user organizational structure; and integration of new TTPs for operation of the system. Other actions may require planning for training of typical users to operate the system and logistical support of the system during the event. Data generation and collection requirements may require identification of new or modified instrumentation for simulation or stimulation of the tested or supporting systems as well as event scenario and control requirements. These and many other actions are necessary to ensure proper event execution that provides credible and usable data to address the evaluation or other customer requirements.

c. The event summary and overall methodology is developed to provide the upper level logic behind the event and how the event will be structured and controlled for generation and collection of data. It identifies the overall design for employment of the system under test and sets the basic parameters for all subsequent planning. There are three basic comparison designs that can be used:

(1) *New versus existing.* When a new system or concept is replacing an existing system or concept the design should be based on a comparison of both systems performing against the same measures and in the same environment. If data are available that shows how the existing system performs against the measures in the required environment, the system evaluator must determine the adequacy of the data and whether additional testing of the existing system is necessary.

(2) *With versus without.* A comparison is made of the unit or organization operating and accomplishing its mission with the system and without the system.

(3) *New versus predetermined standard.* In some cases the standards defined for the system are clear and may be used as the basis for comparison. The new system is tested to see if it meets the predetermined standard.

6–43. Event design

Determining the event duration and sample size required for collection of the required quantity of data is often a difficult process. It requires both an adequate knowledge of the system or concept under test and detailed information on data requirements, environment to be simulated, and player force structure and mission requirements. Event duration and sample size must be based on the minimum amount of testing required to provide data to support customer requirements to reach definitive conclusions concerning the system or concept under test. As such, sample size and event duration requirements are usually derived using a combination of statistical procedures and military judgment.

a. The following paragraphs describe the process for identifying the event factors and conditions that lay the foundation for developing the event design, sample size, and event duration requirements.

(1) *Event variables.* Event variables (factors and conditions) are three types of event variables (often referred to as event factors)—independent, dependent, and uncontrolled. During events, all three types of variables assume discrete values (or conditions). It is the tester's responsibility to control the independent variables in order to measure the response in the dependent variables. Event trial matrices result from combinations of the independent variables that constitute a condition for which data are needed. The data collected under that condition constitutes the dependent variables—the information needed for subsequent system evaluation. An uncontrolled variable is one that is not selected or cannot be controlled by the tester; however, it may have a significant effect on the dependent variable. One of the primary considerations in designing an event is to minimize and/or document the effects caused by extraneous variables.

(2) *Test controls.* The operational tester develops the initial list of event variables and during event planning adjusts the factors and conditions based upon the data required for answering the event issues, criteria, and measures. Factors are controlled in one of four following ways:

(a) Tactically varied factors enhance event realism because the conditions develop as a result of tactical operations employed in the event.

(b) Systematically varied factors are used to permit examination of all required factors in sufficient quantity for effective analysis. The tester establishes the values that the systematically varied factors will obtain during the event.

These are normally the independent variables that the test combines to create specific operational situations under which data must be collected.

(c) Factors are held constant for the test when prior knowledge or testing indicates a preference, or no other option for that factor is available.

(d) Uncontrolled factors should be held to a minimum. When critical factors for a system are identified, the most representative conditions for that factor are developed into the event matrices with the number of conditions held to a minimum.

(3) *Combining conditions.* The selected set of test conditions is used to determine what combinations of conditions are appropriate. For example, a hypothetical system's target detection capability could be influenced by three training level conditions (untrained, average, and highly proficient), three weather conditions (that is, clear, overcast, and precipitation), and two terrain conditions (that is, flat and mountainous). This situation would require consideration of 18 possible test combinations (3 x 3 x 2=18). The radio communications capability of the hypothetical system could require consideration of training and terrain conditions (3 x 2=6 combinations) because weather conditions have little effect. A suggested technique is to draw a matrix listing possible combinations that interact and influence system performance. Normally, systematically varied controlled factors form the basis of this matrix.

(4) *Number of required trials.* The number of required trials for a phase is normally dictated by statistical requirements to answer issues, criteria, or measures. The required sample size is determined numerically by defining statistical parameters and formally calculating the sample size. The system evaluator and operational tester may apply military experience and judgment in determining the total number of trials required when resources or other limitations do not allow for a true statistical sample size. Where there are no statistical criteria, the system evaluator and operational tester must determine how many test trials are necessary to average out chance differences between repetitions of specific events. Essentially, this process determines how many repetitions are required to provide confidence that the event results are valid and representative of a true operational environment. If necessary, the operational tester should document any event limitations resulting from inadequate sample sizes in paragraph 1.5 of the EDP. A trial matrix is developed for each phase or set of requirements to show the number of iterations necessary to achieve the desired level of data collection for each phase.

b. Event planning must always consider the requirement to balance event realism and event control. Test designs that do not include the capability for possible degradation of system performance due to realistic conditions of employment fail to address a critical decision area and can seriously reduce the value of the test results. Event realism comes from scripting the events to follow the OMS/MP and the approved doctrine and TTPs. Event realism is enhanced when the players, friendly and threat, are allowed to respond to the natural battlefield conditions. However, in order to answer the COIC and AI, the event executor must be able to collect the data, which requires that a certain amount of control be maintained during the event trials. The conditions for test environments will normally fall into one of following three categories of operational realism:

(1) *Maximum.* This type of event requires simulation of a tactical environment. A scenario is developed that merges the event trials and activities into a realistic and believable sequence. The scenario describes the actions of all player and opposing forces units and includes all information that will be presented to the players. This type of realism is maintained by including initial and updated briefings for friendly and threat force players through operations orders, fragmentary orders, intelligence summaries, messages, and other information designed to evoke player response. Scenarios are based on standard TRADOC scenarios or other scenarios as specified. The particular scenario to use is agreed upon by the system evaluator and operational tester and the system proponent. In preparing the scenario it is essential to specify the time and location of each planned trial or activity. Once trials begin, there is limited intervention by controllers.

(2) *Limited.* When events do not require maximum operational realism, the preparation of a scenario may be unnecessary. It is, however, necessary to develop a detailed description of the events that will occur. The description should be sufficiently detailed so that the trials or activities can be executed without additional information. For each, the method, time, location, participants, and information to be provided must be specified. Mission event or execution lists may be used to ensure that the required amount of realism is maintained and that the required data are being collected.

(3) *Minimal.* This type of realism may be appropriate for customer tests. Although little realism is simulated in this type of event, there is need for the event executor to maintain close supervision through frequent checks to ensure that the user is properly employing the item or concept. For these tests, this section describes the frequency of checks and inspections and the areas to be checked.

c. Event control procedures must be developed to ensure that the event can be properly organized and executed to generate the required event data. Control procedures vary as to the type and need. For events that have limited or maximum tactical realism, detailed control procedures are normally required to ensure that specific tactical operations

occur, both friendly and opposing forces units begin and generally conduct operations as required, and instrumentation and simulation or stimulation devices are operating as required. Other control procedures may address placement and recovery of data collection personnel, visitor access, logistical support requirements, and other similar items. Regardless of the type of event, necessary control procedures must be identified by event planners and implemented during event execution to ensure that the execution proceeds in accordance with the test design requirements. A control plan is usually developed to identify the specific control measures required and to identify those personnel and situations in which a specific measure must be implemented. This plan normally is included in the event planning documentation.

d. The collection of event data through the use of automated instrumentation systems is a key factor in the majority of events. In addition, instrumentation systems that use M&S are often employed to provide realistic simulation of combat environments (weapons simulator, NBC stimulants, C4I stimulator) and to generate data for systems to use in lieu of having actual forces in the field (combat simulations and stimulation).

(1) *Instrumentation.* Instrumentation planning is conducted to identify those instrumentation systems that are required to collect data to address the event issues and/or to provide the necessary degree of combat environment realism or generation of cue and/or task loading information. The tester identifies the detailed requirements for instrumentation support through the overall data requirements process, test control procedures development, and data collection and reduction planning. The operational tester identifies instrumentation, M&S, and stimulation requirements early to ensure time to procure long-lead items.

(2) *Modeling and simulation and stimulation.* The use of models and simulations is highly recommended and emphasized in operational events. Employment can be used for reducing costs, providing or enhancing test design, predicting results for comparison with field results, providing simulation or stimulation of systems and organizations that cannot be actually present, and assessing areas that cannot be fully tested. However, there are two restrictions on use:

(a) M&S data cannot be the sole source for production decisions in lieu of OT.

(b) All M&S must undergo VV&A prior to use. Simulators, emulators, drivers, and stimulators that are used to fully workload systems under test are included in this category. Threat simulators are a separate category but must also be approved and certified for use.

e. The analytic approach is the methodology by which the event data will be collected and processed to address the event requirements. The methodology must include elements of the following areas: independence (that is, free from bias as possible), comprehensiveness (that is, covering effectiveness, suitability, and survivability to the appropriate level), credibility (that is, believability since a report that is ignored has limited value), validity (that is, addresses the system's mission accomplishment in an operational environments), accuracy (that is, stating the evidence as found), and clarity (that is, getting to the point while not being robust). The methodology for the analytical approach will address the following items:

(1) The methodology is developed based upon the overall product that is required for the customer and is tailored for each event as appropriate. For example, for an oversight system, the event could produce a level 3 authenticated event database that would result in a test data report (TDR). In this case, the event executor would not be responsible for data aggregation at the criterion and issue levels and the analytic approach methodology would focus on how the event executor plans to combine the different sources of data generated during the event into the authenticated test database. For a non-OSD T&E oversight system or for a non-acquisition program event, a Test Report that provides assessments or evaluative information may be produced. In this case, the tester may have the responsibility for aggregating data at the measure, criteria, or issue level to address the customer requirements. In this case, the tester would describe the methods for aggregating the data at the criterion or issue level to address the criterion or issue questions.

(2) The major areas of discussion for the methodology will center on the requirements for the specific issues, criteria, and measures assigned to the event. The tester must be able to explain the relevance of the measures with respect to the criteria and issues and develop the appropriate data collection, reduction, and aggregation methods. Measures must be clearly defined, including unique terms, factors and conditions, and data elements identified. Formulas must also be developed and any deviations from standard formulas identified.

(3) The data collection and reduction procedures required to answer a measure are a function of the degree of precision established for a given measure. Some measures will require input from several sources in order to provide the data to answer the measure. Data from instrumentation, 1553 data bus records, and manually collected data may be combined before the measure can be answered. In other cases, the measure may be answered by a single source of data, for example, a questionnaire provided to the test players. The objective of the data collection, reduction, and aggregation paragraphs under each measure is to provide a clear explanation of how the data is collected, reduced or merged into a data set, and aggregated at the conclusion of the event.

f. Data management planning must address all aspects of requirements for the organization and procedures for data collection and reduction efforts, the critical data process descriptions, DAG requirements, if any, JMEM data requirements, and the event database.

g. PA is a major element in operational event planning. It provides the transition between the measures contained in the approved SEP to the identification of the actual data elements required to calculate and identify a response for the measures. The PA is required for all OT events and becomes an appendix to the EDP. Thus, it is staffed, approved, and distributed as part of the overall requirements for the EDP. The PA is normally prepared in dendritic format and depicts in hierarchical format the relationship of COIC and AI into measures and related specific test and/or evaluation questions, data requirements (additional related questions) and/or data elements. The PA can be displayed in narrative terms or graphically and is normally developed by the event executor. (See fig 6–6.)

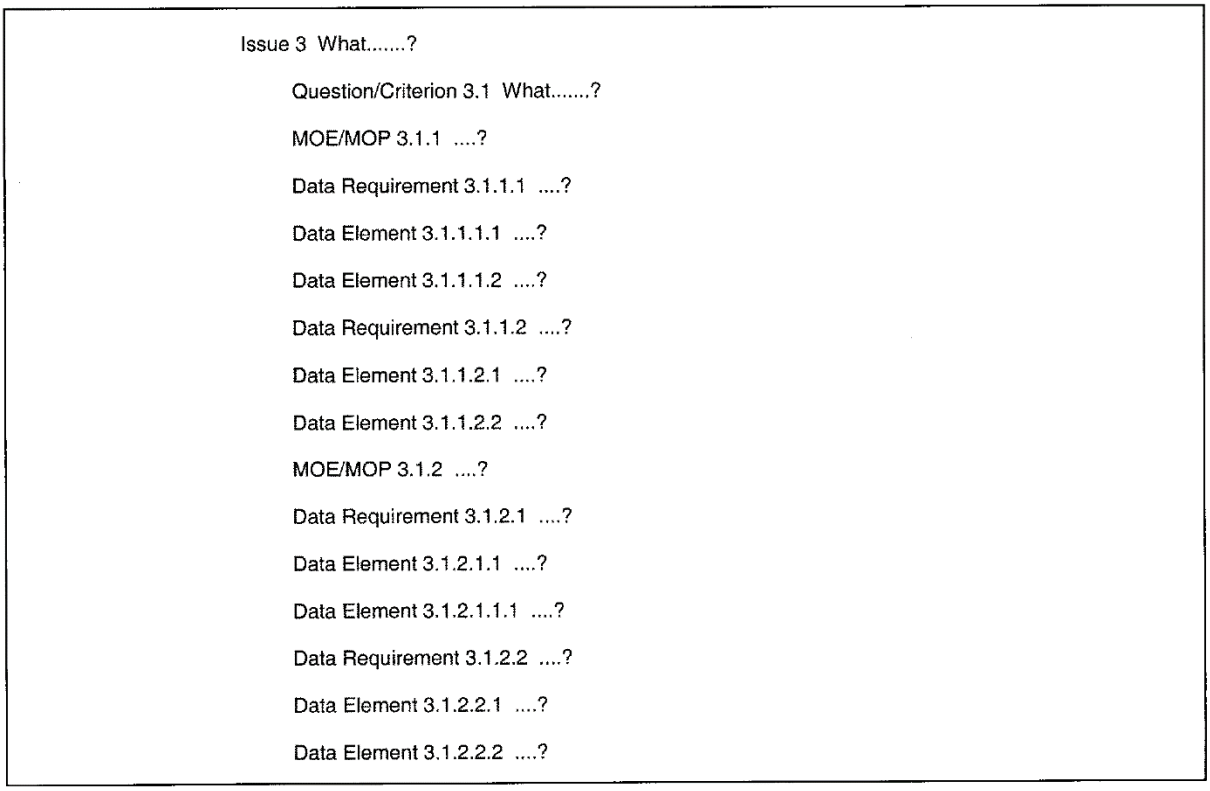


Figure 6–6. Pattern of analysis example format

(1) *Development.* The initial portion of the PA is developed by the system evaluator as a function of the development of the detailed evaluation requirements following approval of the evaluation strategy at the ESR. Using the approved strategy and the COI and AI, the system evaluator develops the initial portion of the dendritic of the PA to organize requirements under the broad areas of operational effectiveness, suitability, and survivability. Each issue or requirements for the issues are assigned to one of the functions of effectiveness, suitability, and survivability as appropriate. Measures are developed to address requirements to answer each issue (without concern as to the data source). This process may suggest that a draft AI could be better incorporated or other draft AI are required. If so, the draft AI should be eliminated as a separate issue. The measures are used by the system evaluator to support development of the required data sources and the DSM. The event executor finalizes the PA and develops the individual data elements by using the measures assigned to a specific event.

(2) *Priority levels.* As part of the process, the system evaluator, in coordination with operational tester, will establish the priority for each measure using the priority levels as shown below. The measure priority assists the operational tester if test resources are subsequently changed necessitating a change in the test design.

(a) Priority 1. Measures required for answering the critical issues of operational effectiveness, suitability, and survivability. Measures that are directed for inclusion by others who approve/disapprove test plans (that is, DUSA (OR) or DOT&E).

(b) Priority 2. Supportive Measures that mitigate the level of risk in answering COI/AI and that address areas resulting from CE lessons, and/or critical mission essential software functions that didn't work well during DT.

(c) Priority 3. Measures that are prudent to collect and support answering the issues (for example, causality or diagnostic).

(d) Priority 4. Measures that are recommended for inclusion by others in the T&E community (for example, AMSAA, PM, or TSM).

(3) *Ultimate goal.* The ultimate goal of the PA is to link COI and AI with simple and measurable data elements. The key to establishing this link, within the process of subdivision, is the identification of each MOE or MOP. MOEs focus on mission accomplishment and military utility. They serve as the higher level measures. MOPs normally can be expressed numerically in observable terms that represent identified dependent variables by which the system performance can be characterized. Data elements are the lowest level of information collected and generally require recording of an item of information that is factual, based upon observation or instrumentation, and require no linkage with any other data element to record. A quality PA is used by the event executor to assist in the planning and development of requirements for the event scenario or other scheduling plan, as well as the data collection and management plan.

h. Operational event date planning requirements are often expressed in relation to the event start date or end date. The OTP and RS milestones are based upon this system. This methodology is used in the event planning and reporting documents. The following test date definitions are provided to preclude any confusion concerning the process:

(1) *Test start date (T-date).* T-date is defined as the date on which data collection for record begins. Pretest training and pilot test activities are accomplished prior to T-date.

(2) *Test end date (E-date).* E-date is defined as the date on which data collection for record is completed. Supporting assets are normally released at or shortly after E-date.

6–44. Entrance criteria for operational testing

Entrance criteria provide a structured mechanism for identifying and reducing risks associated with transitioning from DT to OT. To assist in developing system specific entrance criteria, table 6–3 provides a set of detailed "templates," that can assist in reducing and eliminating risk. Establishment of system specific OT entrance criteria can help document a credible and effective development program. The contents of these templates are not directive and do not supersede existing acquisition guidance. The requirement for certification of system readiness for OT descends from DoDI 5000.02. Detailed information regarding each template is located at appendix X.

Table 6–3
Operational testing entrance criteria matrix of templates

Test planning and documentation	Test planning and documentation	System design and performance	System design and performance	Test assets and support	Test assets and support
Schedule	Concept of operations	Contractor testing	Production rep articles	Test team training	Packaging, handling and transportation
Requirements	TEMP	DT	Interoperability and compatibility	Personnel	Support agreements/ contractor support
AoA	OT				
Event design plan	Live fire testing	Software development	T&E infrastructure	Threat systems	
STAR	Deficiency ID and correction process	System performance	Safety reviews and certifications	M&S	Technical data
Maintenance concept	Security planning	System maturity	Deficiency resolution	Support equipment	CTSF testing
	Configuration management plan			Sufficiency of spares	Joint interoperability testing (if required)

6–45. Operational test readiness review

OTRRs are conducted prior to each OT to allow Commander, ATEC (or other operational test commander) to assess the overall readiness for test of the system. The OTRRs determine readiness of the system, support packages, instrumentation, test planning, and evaluation planning to support the OT. The OTRR includes identification of any problems that impact the start, or adequate execution of, the test and subsequent evaluation or assessment of the system. The objective of the review is to determine if any changes are required in planning, resources, training, equipment, or timing to successfully proceed with the test.

a. Operational test readiness review composition.

(1) OTRRs are chaired by Commander, ATEC; the commander of any other operational test activity; or their designees. The Commander, ATEC chairs all OTRRs for ACAT I, ACAT II, MAIS, and OSD T&E oversight systems. They may delegate the chair for a specific OTRR. Commander, OTC (or other operational test commander) will chair OTRRs for non-major, non-oversight systems and for FDT/E, CEP, and CT. They may delegate the chair for a specific OTRR.

(2) Principal OTRR attendees include the operational tester; system evaluator; PEO, PM, or MATDEV; CBTDEV; TNGDEV; logistician; developmental tester; command providing user troops for test (normally U.S. Army Forces Command); HQDA staff elements; host installation; and contractors.

(3) The operational tester (test director or test officer) will provide planning, administrative support, and reporting results for the OTRR. For ACAT I, II, and all systems on the OSD T&E Oversight List, the tester works in close coordination with the system evaluator to schedule the OTRR and establish the agenda.

b. Operational test readiness review schedule. Three OTRRs are essential for most post-Milestone B operational tests. When necessary, any of the participants may request the chair convene an additional OTRR. An OTRR may not be used for purposes outside its intended scope such as system reviews. Table 6–4 depicts recommended dates for the OTRRs. The three essential OTRRs follow:

Table 6–4
Recommended operational test readiness review dates

Operational test readiness review[1]	Date[2] (days)	Remarks
#1	T–270	Action officer review to identify any restraints to test planning and coordinate corrective actions
#2	T–60	Review adequacy of test readiness prior to approval of deployment of resources to OT site
#3 T–1	Review results of pilot test, to include end-to-end data run, and approve start (or delay) of the OT	

Notes:
[1] Additional OTRRs may be conducted.
[2] T is the OT Start Date

(1) An action officer level review (which is chaired by the operational tester) at approximately 9 months prior to test (T–270). This review focuses on identifying those activities and actions, if any, that appear to be moving too slowly to support the test start date or proper test execution. At this meeting, any misunderstandings on the identity of activities responsible for elements of test planning, readiness, and execution are resolved. For selected high-interest tests, this OTRR may be elevated to a general officer level OTRR.

(2) A review prior to resource (player, testers, and equipment) deployment to test site (normally at T–60). A primary consideration of this review is to ascertain if any known problems exist that would delay test start, and to preclude incurring deployment costs when the test start date is in jeopardy. At this review, resource providers confirm their readiness to release the resources to the tester. MATDEV, CBTDEV, TNGDEV, and test unit operational test readiness statement (OTRS) are provided to the tester at this review. The safety release should be provided at this OTRR, but if not, it must be provided prior to beginning of hands on training of test players. For all templates, a color-coded summary status should be provided. For incomplete, open template line items (that is, red or amber) the PM must provide a separate briefing slide indicating status and/or corrective action plan.

(3) A review prior to the beginning of record test in order to determine if the tested system, players, testers, instrumentation, targets, and threat simulators (ITTS), and data reduction procedures are ready for testing for record. This

OTRR is normally conducted at the test site during latter phases of, or immediately following, the pilot test. In addition to topics addressed during previous reviews, data collection and data reduction techniques, functions of automatic data processing systems, validity of pilot test data, and operations of the DAG, if appropriate, are examined. The test officer and the system evaluator confirm the success of end-to-end data runs.

c. Pre-operational test readiness review. A pre-OTRR is normally conducted the day prior to the official OTRR. The pre-OTRR is an action officer level meeting that attempts to reduce known problems by developing solutions and milestones prior to the OTRR. Normally, only matters that could prevent valid testing (potential showstoppers) are briefed at the OTRR. In those cases where the T–270 OTRR is conducted at the action officer level, there is no need for a pre-OTRR.

d. Operational test readiness review product. The resultant product of each OTRR is a decision by the chairperson to execute the OT as planned, to direct required changes to ensure successful test execution, or to recommend (to the program decision authority) delay or cancellation of OT. Start of the OT will be delayed when a problem is identified that would affect the validity of the data being collected to address the evaluation issues. OT start can also be delayed when it is apparent that the system has little chance of successfully attaining CTPs or satisfying critical operational criteria, and deficiencies cannot be resolved before the start of the test. OT may also be delayed when it becomes evident that critical test data or information cannot be obtained to adequately answer the issues. (See AR 73–1.)

e. Operational test readiness review preparation. OTRR preparation includes the following:

(1) The OT activity will be responsible for scheduling the OTRR. Attendees will be notified of a scheduled OTRR and the planned agenda at least 30 days prior to the review.

(2) A typical OTRR agenda is provided at figure 6–7. It should be used as a guide in developing an appropriate agenda for a particular system. Mandatory subjects for briefing by the tester at all OTRRs are specifically identified. The agenda should always include provisions for the MATDEV, CBTDEV, TNGDEV, and test unit commander to provide their OTRS, which formally addresses system readiness for OT. Additionally, prior to OT to support the FRP DR, the PM certifies the system is ready for a dedicated phase of OT. The status of any incomplete OT Entrance Criteria Template.

f. Minutes. Minutes of an OTRR are distributed to OTRR participants within 10 working days after adjournment of the OTRR. Within 3 working days after adjournment of the OTRR, external commands or agencies are notified by either message or memorandum of any issues or problems surfaced during the OTRR for which their agency has responsibility for resolving prior to test start. The message may solicit the personal assistance of the agency commander in overseeing necessary corrective actions. Within 5 working days after adjournment of the OTRR, a status report outlining the results of the OTRR is provided to the appropriate decision makers. The format and addressees are determined on a case-by-case basis by the chairperson, based on the outcome of the review and degree of assistance required to resolve outstanding issues.

6–46. Operational test readiness statement requirements

a. As a prerequisite for test initiation and prior to the start of the test, the MATDEV, CBTDEV, TNGDEV, and test player unit commander each provide the operational tester with a written statement of the system's readiness for OT. The operational tester specifies in the OTP milestone schedule the suspense dates for the OTRS (normally 60 days prior to the test start date).

b. Deviations from the required readiness standards for test (such as system safety and training) require a statement of explanation by the OTRS proponent (such as MATDEV, CBTDEV, and/or TNGDEV).

c. For ACAT I and II system OTs conducted in support of the FRP DR, the MATDEV OTRS must certify that the system is ready for a dedicated phase of OT&E. (See DoDI 5000.02.)

d. The system evaluator and operational tester review the OTRS to ensure that identified deficiencies will not affect the ability of the OT to answer the evaluation issues.

e. For OTs not conducted by ATEC, information copies of the OTRS are provided to ATEC. An OT will not be initiated until all OTRSs have been received and reviewed by ATEC.

f. Types of OTRSs include—

(1) MATDEV OTRS.

(a) The MATDEV describes the system to be tested in terms of size, shape, weight, transportability, and functional characteristics.

(b) For software-intensive systems, the MATDEV specifies the software version to be tested and current documentation to be made available. A detailed statement of how both the system hardware and software characteristics differ from a fully representative IOC system is provided, where appropriate.

(c) The MATDEV identifies the DT objectives that have been met and all failures and deficiencies that have been corrected. Any DT objectives not met or failures not corrected will be detailed, and estimates of their effect on OT described.

(d) The MATDEV identifies special instrumentation required and the availability of that instrumentation through their office.

(e) The MATDEV identifies the system maintenance, training, and supply resources requirements that are to be evaluated during test. Military resupply procedures, support procedures, and special support requirements are defined. If system contractor support is called for, the specific role of the system contractor is defined at each echelon.

(f) The MATDEV estimates the current and projected RAM performance in terms of the system ORD.

(g) The MATDEV includes a detailed statement concerning any restrictions to ordinary operations under field conditions that will exist in the test.

(h) The MATDEV provides a safety release for the system (obtained from ATEC's DTC) or identifies the status of the release.

(i) The MATDEV includes a mission impact analysis of unmet criteria, including critical interoperability problems to be assessed during the OT.

(j) The MATDEV certifies and accredits communications system per DoDI 8510.01.

(k) The MATDEV includes the results of the Environment, Safety, and Occupational Health review.

Operational Test Readiness Review Agenda

1. **Purpose**

2. **Program Sponsor Issues** (Program Sponsor)
   a. Results of Previous Testing.
   b. System Equipment Status.
   c. Operational Test Readiness Statement.
   d. Safety Release.
   e. System Delivery Schedules (Milestone).
   f. Contractors Support.
   g. Logistics Support Plan.
   h. Instrumentation.
   i. System Transfer Plan.
   j. Certification of Systems Readiness for OT.
   k. Certification that software design is stable.
   l. Other Special Topics, such as information assurance.

3. **Combat Developer/Trainer Issues** (Combat Developer/Trainer)
   a. Test Soldier Training Results.
   b. Operational Test Readiness Statement.
   c. Safety Release.
   d. Logistic Concept.
   e. Operational Mode Summary/Mission Profile.
   f. Threat.
   g. Test Setting.
   h. Certification for System Readiness for OT.
   i. Other Special Topics.

4. **Test Readiness** (Operational Tester)
   a. Test Directorate Organization (Mandatory). Description of the overall test organization and structure for the test.
   b. OTP Resources/FORSCOM Support (Mandatory). Status of support required/received or coordinated in accordance with OTP.
   c. System Evaluation Plan/Event Design Plan/Detailed Test Plan (Mandatory). Overview of the test design to include issues and criteria as appropriate and status of SEP development.
   d. Test Schedule (Mandatory).
   e. Participation/Other Agencies.
   f. Pilot Test (Plan or Result) (Mandatory). Description of planning pilot test activities or results of the pilot test.
   g. Data Displays.
   h. Data Collection Reduction and Processing Plan.
   i. Test Instrumentation Status.
   j. Threat representation.
   k. Test Site Support Plan.
   l. Human factors.
   m. Status of MOUs.
   n. Other Special Topics, such as information assurance.

5. **Overall Readiness** (System Evaluator)
   a. Evaluator Critique of System Readiness.
   b. Evaluator Critique of Tactics, Techniques, and Doctrine.
   c. Evaluator Critique of Threat.
   d. Evaluator Critique of Training Readiness.
   e. Evaluator Critique of Test Readiness.

Figure 6–7. Sample operational test readiness review agenda

f. SEP Status.
g. Overall Evaluation.

6. **DAG Composition and Operation** (Operational Tester)

7. **ADP Plan** (Operational Tester)

8. **Funding** (Operational Tester)

9. **Identification and Review of Showstoppers or Potential Showstoppers** (Operational Tester and Evaluator)

10. **Review of Action Items** (Operational Tester)

11. **Discussion** (All)

12. **Decision** (Chairman)

Figure 6–7. Sample operational test readiness review agenda—Continued

(2) *Combat developer operational test readiness statement.* The CBTDEV OTRS verifies that the doctrine, organization, threat, logistics concept, crew drill, and SOPs in the CBTDEV's support packages are complete, represent planned employment, and are approved for use during OT.

(3) *Training developer operational test readiness statement.* The TNGDEV OTRS verifies that the training concepts and materiel and crew drills included in the training support package are complete, representative of the training package to be used at fielding, and approved by TRADOC for use during OT. In addition, it verifies that the user troops have satisfactorily completed training in accordance with the training support package and are ready for test.

(4) *Test unit operational test readiness statement.* A signed OTRS is required from the test unit commander. This statement certifies that unit personnel are Military Occupational Specialty qualified and where appropriate, the test unit can perform the required External Evaluation tasks. This statement does not certify that unit personnel are trained on the test item.

6–47. Safety release for operational testing

a. A written system safety release obtained from ATEC's DTC must be on hand prior to initiating any training or testing involving user troops. The test officer must ensure TRADOC proponent schools and all test directorate and test player personnel know safety precautions and procedures. At OTRR #2 (T–60), the program sponsor or other agency responsible for the safety release will provide it to the test officer.

b. ATEC's DTC is responsible for issuing the safety release (see AR 385–10) for all materiel systems being tested, including type classified materiel if the materiel is to be used in a new or innovative manner. Exceptions to this policy are systems being developed by USAMEDCOM. The program sponsor must submit requests for the safety release to ATEC's DTC as soon as the requirement is known, along with all data available regarding the item. When sufficient data are not available on which to base a safety release, it may be necessary to conduct additional testing. If required, the developer will pay test costs and the time required for issuing a safety release will increase accordingly. Funding for any required testing will be included in the OTP. To assure timely receipt of the safety release, the operational tester must proactively coordinate with the activity responsible as soon as the requirement is known.

c. A copy of the safety release is provided to the commander of the organization supplying the troops to ensure that the organization is informed of the identified risks. For weapon systems, both live fire and non-fire safety releases may be required.

d. Where appropriate, the safety release indicates the results of The Surgeon General's Center for Health Promotion and Preventive Medicine (CHPPM) investigation of medical or health problems related to the materiel system and include a certification as to the safety of user troops. Operational tests using aircraft require an airworthiness release. (See AR 70–62.)

6–48. Delay or termination of operational testing

a. In the event that an OTRR indicates that testing should be delayed (for example, inadequacies of SSPs, OTRSs, training, test planning, instrumentation, and so forth that will adversely affect test start, execution, or its realism and/or completeness), alternative courses of action and recommendations are developed that, if executed, assist in maintaining the integrity of the test.

b. Due to the TSARC 1-year notification requirements for provision of resources for support of OT, a seemingly short delay in the start of the OT could result in a delay of a year or more. (See AR 73–1.)

c. If a determination is made that suspension of testing is necessary, the chairperson expeditiously forwards the issues and recommendations to the decision authority, with information copies to the milestone DR principals, for a decision to start, delay, or terminate the test.

6–49. Operational test pretest activities

These activities involve all pretest training, organizing for execution and support, preparation of equipment and test areas, the pilot test, adjustment of plans (if necessary), and all other actions required to prepare for the test. The training plan and support plan are of major interest during these activities.

a. Training phase.

(1) Regardless of the type of test, some evaluation of training and training support is normally conducted. This is necessary to ensure the skills and knowledge necessary to operate and maintain the system can be attained and sustained within realistic training environments by units using personnel of the type and qualification expected when the system is deployed. When training is an issue, MANPRINT and training data collection must begin prior to T-date (in other words, at the start of player training).

(2) Conducting NET is the MATDEV's responsibility. NET transfers knowledge gained during materiel development to trainers, users, and support personnel during development and fielding of new equipment. The contents of the NET TSP are described in paragraph 6–60.

(3) TRADOC provides for the analysis, design, development, implementation, and control of resident training programs and exportable training products. The TRADOC school responsible for the Military Occupational Specialty affected by the test item will prepare a training TSP.

(4) The extent of training and training support evaluations is contingent on the test type and stage of development of the system being tested. Ordinarily, training is contractor administered in the early phases of materiel development. For subsequent phases, the MATDEV provides training to military instructor personnel, who then train test participants. The objective, however, remains the same: to assess the adequacy of training associated with fielding the system.

(5) Test officers ensure that test directorate and player personnel are adequately trained. This often requires coordination with support divisions and TRADOC proponent schools. It is also important to ensure that test player personnel satisfy test requirements in terms of Military Occupational Specialty and skill level. Training includes that necessary for controllers, support personnel, data collectors, and data reducers.

(6) Training conducted in support of tests will include training individuals, crews, and units in individual and collective tasks required to employ the system in accordance with approved doctrine and tactics. Training will be in accordance with the TSP and representative of that intended to support the system when initially fielded. The proponent TRADOC school must provide the test organization and Headquarters, OTC with certification stating test players have been trained and can perform individual and collective tasks to standard in accordance with the milestone schedule in the OTP. This written statement constitutes one element of the OTRS but is provided separately from other elements of the TNGDEV's OTRS.

(7) All training provided to player personnel, any performance problems during the test attributable to inadequate training, and comments of personnel who received the training must be recorded and subsequently analyzed.

(8) Data are collected during the training phase if required by the SEP. If the SEP does not require training phase data, the test officer may wish to collect these data as a training device for data management personnel and as an opportunity to perform an end-to-end data run.

b. Support. Adequate support is essential to any test execution. The test officer must ensure that all logistical and administrative requirements that are planned or becomes necessary for the test execution are properly performed. The requirements and plans for support are documented in the OTP for the test.

c. Operational test pilot test phase.

(1) A pilot test is an abbreviated version of the actual test and is conducted in advance to detect deficiencies in the plan, instrumentation, data collection, data management, and test control. It includes the exercise of each type of required event and makes use of each data collection means. It is essential that the complete data management procedure, to include DAG operational procedures in accordance with the DAG SOP, be verified as a part of the pilot test.

(2) The pilot test is addressed in the EDP with sufficient time between pilot test and the start date of the actual test so as to allow for identification of, reaction to, and correction of any deficiencies encountered. Tests relying heavily on instrumentation may require additional time after the pilot test for the correction of problems. Accomplishment of an abbreviated program of events is usually sufficient, although an abbreviated control procedure may also be required.

(3) If a pilot test is not required, it is to be explicitly stated in the SEP. When extensive training of player personnel is required, a pilot test may be conducted concurrently with the training test phase.

(4) Problems revealed during the pilot test are to be corrected prior to the actual test. This may involve the conduct of additional training, identification of additional support, resources, changes to the EDP, or revision to the SEP.

(5) The length of the pilot test must permit the exercise of every type of major event required in the test, as well as every type of data collection instrument to be used. There should be enough workdays between the end of the pilot test and actual T-date to incorporate any necessary changes.

(6) Test directorate organizations must duplicate those conditions envisioned for the actual test and all directorate members must participate. The degree of player participation must be tempered by considering if learning during the pilot test would bias results of the actual test.

(7) Data should be collected and reduced in the same manner by the same personnel to be used during the actual test. A complete end-to-end data run must be conducted. This starts with test events and goes through every step until the created test database is accessed.

(8) All manual data collection forms must be validated and all instrumentation, from stopwatches to computers, used. The need for filming test events should be carefully reviewed. Video tape is an excellent way to record data; however, the data reduction and analysis effort associated with this medium can be lengthy and tedious.

(9) If the test involves a two-shift operation, data review procedures must be established and validated during the pilot test.

(a) One of the best methods of injecting quality control into the data collection effort is for the data manager or assistant data manager to be present at the shift change to review collected information. Temporary data collection forms may be created for each specific test conducted, based upon the specific requirements of the test and the characteristics and requirements of the system under test. The completed forms need to provide complete data, legible narrative comments, and be dated and signed.

(b) Incomplete forms indicate the data collector does not understand the job or is not interested in doing the job right. In either case, the problem must be resolved prior to the test commencement.

(c) The conduct of data reviews and debriefings at shift changes is essential.

(10) Upon completion of the pilot test, all test directorate personnel should be critiqued on their performance and encouraged to ask questions and discuss problems they encountered. It is essential for all test directorate personnel to understand their responsibilities and to know whom to contact should a problem occur.

(11) Adjustments may be required to correct deficiencies revealed. This may involve conducting additional training, requesting additional support, revising control procedures, altering the test directorate organization, and revising data collection forms.

(12) All problems surfaced during the pilot test must be addressed. They will not go away during actual testing. All issues will be discussed and resolved at OTRR #3. This review will give the go-ahead to start the test.

(13) Contingent upon the desires of the system evaluator, data collected during training and the pilot test may, or may not, be considered valid. This is particularly true for RAM data. Use of these data should be in accordance with the approved SEP and associated FD/SC. These data must be comparable and compatible with the data from record trials. If any of the data from the pilot test are used as data in the test report, the data must be obtained under the same test conditions as the record trials.

6–50. Data authentication group operations

The DAG authenticates and validates the test data, ensuring that test data accurately reflect the system performance during the test and provide the single test database of record (the ground truth) for all users of the test data. The DAG identifies and analyzes anomalies in the system under test, instrumentation, and test data. The DAG provides interested agencies a conduit to express opinions during test planning and execution.

a. Establishment of the data authentication group. The system evaluator establishes the requirements for a DAG on full-evaluation system tests. These requirements are documented in the SEP. If the system evaluator does not

require a DAG, the tester determines if a need exists and establishes a DAG accordingly. The tester also determines if a need exists and establishes a DAG for an abbreviated evaluation system and for FDT/E, CEP, and CT.

b. Data authentication group. DAG roles and missions include—

(1) The DAG brings together the interested parties on an operational test and allows these parties to view test planning, execution, and data reduction. DAG members provide recommendations to the system evaluator and tester on matters of test design, test conduct, and test data reduction. It provides a level of quality assurance above that expected from the data management/quality control function. The DAG acts as advisory group to the test director and the system evaluator.

(2) Due to the variations in development systems, evaluation strategies, test designs, and data collection efforts, the duties of each DAG are specifically tailored to accommodate the unique requirements of the test. The system evaluator and the tester carefully define the relationship between the DAG and the other elements of the test directorate.

(3) The DAG acts independently of the data management and quality control process and does not work under the supervision of the data manager.

(4) DAG members will review and authenticate the test conduct, data collection, data reduction, and database contents as indicated by the DAG SOP. The DAG will identify and investigate any problems, discrepancies, or anomalies found in these areas, and make recommendations to the test director for resolution of these problems. The DAG verifies that the data contained in performance, human factors, and RAM test databases are valid test results. The DAG will publish reports as required. The DAG serves to promote T&E and acquisition communities understanding and acceptance of the operational test data.

(5) Final decisions on test design, test conduct, and test data reduction lie solely with the tester and system evaluator.

(6) The following values provide a moral compass for the DAG:

(a) Warfighter comes first. Acknowledges that the user relies on the DAG to ensure that the event data reported reflects the demonstrated capabilities of the system.

(b) Truth. DAG remains objective while using all available and appropriate sources of information tempered with credible military and engineering judgment.

(c) Total system. DAG examines all aspects of the total system to include the human and environmental elements.

(d) Value added. While being in a unique position to identify deficiencies and shortfalls, DAG will ensure timely feedback to the CBTDEV or MATDEV or PM so as to identify proper fixes.

(e) Responsiveness. Within reason, DAG should strive to accommodate a program's schedule or unique considerations.

(f) Cost effectiveness. To the extent possible, DAG should economize wherever possible while producing a credible product.

(g) Independence. DAG will let nothing interfere or jeopardize their integrity in accomplishing their mission.

(h) Minimal intrusion. Within the demands for obtaining valid findings, DAG will minimize obtrusion to the test conduct.

c. Data authentication group membership. Membership includes—

(1) The tester normally chairs the DAG.

(2) The DAG Charter establishes DAG membership. Mandatory members are the system evaluator and tester. Other members are selected from the CBTDEV, MATDEV, developmental tester, and other members of the acquisition team. Membership is extended to any pertinent Government agency (for example, DOT&E, AAA, Government Accountability Office) with a vested interest in the system under test. The members of the DAG represent a broad spectrum of technical disciplines and system expertise.

(3) Each DAG is organized to accommodate the unique requirements of the test. Large DAGs are typically organized into various functional teams such as a performance validation team, a MANPRINT data validation team, a RAM data validation team, and a research cell. Small DAGs may consist of one cell.

(4) Section 4171 of Title 10 of the USC prohibits system contractors from direct participation in the DAG for MDAP programs. The DAG permits no system contractor manipulation or influence during IOT and other activities that provide input for consideration during and beyond LRIP decisions for ACAT I and II systems. While system contractor personnel will not attend or be directly involved as members or observers in any DAG sessions, they can be relied upon as technical subject matter experts.

(5) Support contractors to DAG members may participate in the DAG if they have never had a contractual relationship to the system contractor on the system under test.

d. Resources. All resources for the functions of the DAG must be included in the OTP for the test. The tester must estimate resources for personnel, travel, equipment, facilities, and overtime, with input from the system evaluator.

e. Training. The DAG cannot function properly if the members do not have adequate training. Training should be addressed in the DAG SOP and, as a minimum, members should have training in operations and capabilities of the system under test, familiarization with test purpose and concept as documented in the SEP and EDP, the data reduction plan and instrumentation for the test, the DAG SOP, and test organization and key personnel.

f. Data levels. Data levels include—

(1) The originator of the requirement for the DAG determines the data levels to be reviewed by the DAG and addresses this in the DAG SOP. Each member of the DAG should be clear on the meanings of each data level as given in table 6–5.

(2) The DAG SOP may call for examination of data from levels 1–3 in the authentication process. Once the level 3 database has been reviewed and approved by the DAG, it becomes the authenticated database, which is the database of record for that test. Timely release of authenticated level 3 data to members of the acquisition team is highly encouraged. Release of less than authenticated level 3 data will be handled on a case-by-case basis.

(3) The analysts can reduce and analyze these data into findings and assessments (levels 4, 5, 6, and 7).

Table 6–5
Levels of data

Level	Description	Possible forms	Example of content	Disposition
Level 1 "Raw Data"	Data in their original form. Results of field trials just as recorded.	Complete data collection sheets, exposed camera film, voice recording tapes, original instrumentation magnetic tape or printouts, original videotapes, completed questionnaires, and/or interview notes.	1. All reported target presentations and detection. 2. Clock times of all events. 3. Azimuth and vertical angle from each flash base for each flash. 4. Recording tapes of interviews.	Accumulated during trials for processing. Usually discarded after use. Not published.
Level 2 "Reduced Data"	Data taken from the raw form and consolidated. Invalid or unnecessary data points deleted. Trials declared "No Test" deleted.	Confirmed and corrected data collection sheets, film with extraneous footage deleted, corrected tapes or printouts, and original raw data with "No Test" events marked out.	1. Record of all valid detections. 2. Start and stop times of all applicable events. 3. Computed impact points of each round flashed. 4. Confirmed interview records.	Produced during processing. Usually discarded after use. Not published.
Level 3 "Ordered Data"	Data that have been checked for accuracy and arranged in convenient order for handling. Operations limited to counting and elementary arithmetic.	Spread sheet, tables, typed lists, ordered and labeled printouts, purified and ordered tape, edited film, or edited magnetic tapes.	1. Counts of detections arranged in sets showing conditions under which detections occurred. 2. Elapsed times by type of event. 3. Impact points of rounds by condition under which fired. 4. Interview comments categorized by type.	Not usually published but made available to analysts. Usually stored in institutional databanks. All or part may be published as supplements to the test report.
Level 4 "Findings" or "Summary Statistics"	Data that have been summarized by elementary mathematical operations. Operations limited to descriptive summaries without judgments or inferences. Does not go beyond what was	Tables or graphs showing totals, means, medians, modes, maximums, minimums, quartiles, deciles, percentiles, curves, or standard deviations. Qualitative data in form of lists,	1. Percentage of presentations detected. 2. Mean elapsed times. 3. Calculated probable errors about the centers of impact. 4. Bar graph showing relative frequency of each category of	Published as the basic factual findings of the test.

Table 6–5
Levels of data—Continued

	observed in the test.	histograms, counts by type, or summary statements.	comment.	
Level 5 "Analysis" or "Inferential Statistics"	Data resulting from statistical tests of hypothesis or interval estimation. Execution of planned analysis data. Includes both comparisons and statistical significance levels. Judgments limited to analysts' selection of techniques and significant levels.	Results of primary statistical techniques such as T-tests, Chi-square, F-test, analysis of variance, regression analysis, contingency table analyses and other associated confidence levels. Follow-on tests of hypotheses arising from results of earlier analysis, or fallback to alternate nonparametric technique when distribution of data does not support assumption of normality. Qualitative data in the form of prevailing consensus.	1. Inferred probability of detection with its confidence interval. 2. Significance of difference between two mean elapsed times. 3. Significance of difference between observed probable error and criterion threshold. 4. Magnitude of difference between categories of comments.	Published in SERs. If SER is part of test report, the level 5 analysis results are presented separately from the level 4 findings.
Level 6 "Extended analysis" or operations	Data resulting from further analytic treatment going beyond primary statistical analysis, combination of analytic results from different sources, or exercise of simulation or models. Judgments limited to analysts' choices only.	Insertion of test data into a computational model or a combat simulation, aggregation of data from different sources observing required disciplines, curve fitting and other analytic generalization, or other operations research techniques such as application of queuing theory, inventory theory, cost analysis, or decision analysis techniques.	1. Computation of probability of hit based on target detection data from test combined with separate data or probability of hit given a detection. 2. Exercise of attrition model using empirical test times distribution. 3. Determination of whether a trend can be identified from correlation of flash base accuracy data under stated conditions from different sources. 4. Delphi technique treatment of consensus of interview comments.	Published as appropriate in SERs.
Level 7 "Conclusion" or Evaluation	Data conclusions resulting from applying evaluative military judgments to analytic results.	Stated conclusions as to issues, position statements, and challenges to validity or analysis.	1. Conclusion as to whether probability of detection is adequate. 2. Conclusion as to timeliness of system performance. 3. Conclusion as to military value of flash base accuracy. 4. Conclusion as to main problems identified by interviewees.	Published as the basic evaluative conclusions of SERs.

6–51. System contractor relations

a. The intent of 10 USC 4171 is to ensure that, during IOT, major defense acquisition systems are operated, maintained, and otherwise supported by personnel typical of those who will carry out such functions when the system is deployed in combat. (See AR 73–1.)

b. To ensure there is no system contractor manipulation and/or influence during IOT or related activities which provide input for consideration in the system evaluation leading to a FRP DR, system contractor personnel will not—

(1) Participate, except to the extent they are involved in the operation, maintenance, and other support of the system when it is deployed in combat or other normal use (for example, training or instrumentation).

(2) Establish criteria for data collection, performance assessment, or evaluation activities for OT data.

(3) Participate in collecting, reducing, processing, authenticating, scoring, assessing, analyzing, or evaluating OT test data.

(4) Attend or be directly involved as members or observers in DAG sessions (see para 6–52) or in RAM scoring or assessment conferences that address data supporting evaluation or assessment of their systems.

c. Discussions with system contractor personnel may be necessary to ensure full technical understanding of test incidents observed during the IOT&E or related activities. All discussions will be held separately from any scoring or assessment activities. The MATDEV should maintain written record of the nature of these contractor and Government discussions.

d. Since some systems will be maintained by contractors after fielding, it is imperative that any contractor effort be defined in writing prior to T-date. Ideally, any authorized contractor maintenance would be specified by level and extent in each of the appropriate test support packages. Contractor efforts should be an agenda item briefed at the T–60 OTRR, and agreed to by all parties. EUT and FDT/E prior to IOT&E will often require a greater amount of contractor maintenance support, but this must be worked out in the T&E WIPT.

6–52. Release of operational test information

a. Release of OT data to members of the acquisition team (that is, MATDEV, CBTDEV, and TNGDEV) is authorized as soon as the Level 3 data are authenticated. Release is also authorized to TEMA; DUSA (OR); DOT&E, and OUSD (AT&L) Strategic and Tactical Systems; DT&E. The operational tester is authorized to release these data. The release of emerging test results should be provided to the MATDEV as early as possible so that maintenance releases can be accomplished using available data before official release of the report. (See DoDI 5000.02.)

b. Release of OT data beyond the acquisition team will be accomplished only with the approval of CG, ATEC or the commander of other OT&E activities. All such requests for data must be coordinated with the tester, system evaluator, and PEO/PM.

c. The conduct of operational tests on new materiel has gained widespread interest, resulting in numerous requests for interim OT data. These requests are generated by congressional survey and investigative committees, Government Accountability Office, AAA, industry, contractors, and private individuals.

d. Any requests for test information received by the test team from members of news media or civic organizations should be reported immediately to the appropriate agency public affairs officer. Requests for information from private industry or individuals will be processed as public information releases or Freedom of Information Act requests. Directives addressing the release of information must be used for guidance. (See AR 1–20.)

e. Release of draft or interim test reports, system evaluations, or SAs is to be handled on a case-by-case basis, given the level of interest and direction by HQDA, OSD, and the Congress. Assessments made prior to the complete analysis of test results can be very misleading. Such assessments can be found to be incorrect when the complete set of test data is thoroughly analyzed. Moreover, an assessment based upon an incomplete set of test data can cause biases that are difficult to overcome, even when further information proves the initial analysis to be correct.

f. Release of interim data or reports outside of the acquisition team will require—

(1) Requesting agency providing written or verbal request for data to Commander, ATEC or other designated OT&E agency. Expeditious requests may be made via facsimile or phone.

(2) Verification of the requester's identity and need.

(3) Assessment of any difficulties associated with providing the information requested.

(4) Coordination with OT&E agency staff may be accomplished in the most efficient manner possible, such as telephonically, email, or facsimile.

(5) Provision of funding necessary for duplication of large or complex database information.

(6) A transmittal letter stating limitations and caveats and an explanation that this is interim data and should not be used to develop conclusions.

g. All data released will be as authenticated (that is, validated) and complete as possible. The data or report will be clearly marked as interim and cautions to be considered in using it will also be stated.

h. Copies of the release letter will be retained in the official system file.

i. Release of information to system contractors will be made only through the PEO, PM, or appropriate MATDEV representative. Release of information to support contractors will be made only through the contracting officer's representative or contracting officer's technical representative.

j. Security classification and procedures to protect classified or competition-sensitive information will always be observed.

k. Timely reporting of test results is essential and is accomplished through TIRs as well as the formal test reporting procedures. Test incident data are prepared by the operational test organization to provide the results of any incident occurring during testing. In response, as a minimum, the MATDEV prepares corrective action data for all critical or major TIRs. Corrective action data reflect the developer's analysis of the problem and the status or description of the corrective action. All data are put into the ATIRS to enhance the CE of the program. (See app V.)

6–53. Operational test report

A test report is the end product of every test. For those tests in support of the acquisition system, the test report supports the SER, or SA, and provides results of the OT to decision makers, to other interested members of the acquisition team, and to archives, such as the Defense Technical Information Center, for future researchers. For those tests not in direct support of an acquisition system, the test report stands alone as the report of the test effort and provides detailed results to the test sponsor, to other interested activities, and to archives. The test commander or designee prepares the test report. An authenticated level database is provided to the system evaluator and, when requested, to other acquisition team members prior to the approval of the test report to support analytical requirements.

6–54. Test data report

The TDR is an alternative type of report of test results. It is supported by distribution of an authenticated level 3 database prior to its approval.

Section IV

Test Support Packages

6–55. Test support packages overview

TSPs are provided to support conduct of Army testing for new systems undergoing development and fielding. TSPs are primarily used during DT and OT prior to the FRP DR. TSPs include the System Support Package, NET TSP, Doctrinal and Organizational TSP, training TSP, and threat TSP.

a. System support package. The SSP is a set of support elements (that is, support equipment, manuals, expendables, spares and repair parts, and TMDE) planned for a system in the operational (deployed) environment, provided before DT and OT and tested and evaluated during DT and OT to determine the adequacy of the planned support capability. The SSP is provided by the PEO (or PM or MATDEV). An SSP is required for all systems (that is, materiel and C4I/IT). (See AR 700–127.)

b. New equipment training test support package. A NET program is first prepared by the PEO, PM, or MATDEV with input from the TNGDEV in accordance with AR 350–1 to support training development for new materiel and C4I/IT systems, including conduct of test of new equipment and software. Based on the NET program, the PEO, PM, or MATDEV prepares, as appropriate, a NET TSP. The NET TSP is provided to the TNGDEVs and testers. It is used to train player personnel for DT and to conduct training of instructor and key personnel who train player personnel for OT. The TNGDEV uses the NET TSP to develop the training TSP.

c. Doctrinal and organizational test support package. The D&O TSP is a set of documentation prepared or revised by the CBTDEV for each OT supporting a milestone decision. Paragraphs or elements in the D&O TSP not needed (as determined by CBTDEV) will be annotated as "not required" in the D&O TSP. Major components of the D&O TSP are means of employment, organization, logistics concepts, OMS/MP, and test setting.

d. Threat test support package. The threat TSP is a document or set of documents that provides a description of the threat that the new system will be tested against. A threat TSP is required for all materiel systems. (See AR 381–11.)

e. Training test support package. The training TSP consists of materials used by the TNGDEV to train test players and by the system evaluator in evaluating training on a new system. This includes training of doctrine and tactics for the system and maintenance on the system. It focuses on the performance of specific individual and collective tasks during OT of a new system. The proponent trainer prepares the training TSP.

6–56. Test support package applicability

TSPs are required to support testing of all systems (including NDI and modification programs) when they are scheduled for delivery by the responsible organizations in the approved OTP (see AR 73–1) for the test. The TSARC is the appropriate forum to resolve issues regarding applicability of any TSP deemed necessary by the tester when preparing the OTP.

a. The SSP is required to support DT and OT for all materiel systems and tactical C4I/IT systems unless waived. (See AR 700–127.)

b. The PM/PEO/MATDEV of the system conducts NET in support of the developmental and operational testers, and trainers of operational test players, for all systems. NET applies to operations and maintenance of equipment, including software updates and associated documentation. The NET TSP provides this information transfer to the trainer.

c. A Threat SSP is required in support of developmental and OT for all materiel systems when the T&E WIPT determines that an operationally realistic threat is needed for the test. (See AR 381–11.)

d. While the D&O TSP, NET TSP, and training TSP are normally critical to the conduct of testing, they are not mandatory and may not be desired when conditions exist that do not require them.

6–57. System support package

The SSP is a composite of support equipment and documentation that will be evaluated during LD and tested and certified during developmental and operational tests including repair parts, tools, maintenance and training manuals, and consumable supplies. For non-tactical C4/IT and space systems, an SSP is prepared for hardware and software. The SSP is to be differentiated from other logistic support resources and services required for initiating the test and maintaining test continuity (for example, the OTP).

a. Content, policy, responsibilities, and other provisions. See AR 700–127 for content of SSPs, and for associated policy, responsibilities, and waiver provisions.

b. Simulation support plan processes and procedures. The SSP is a composite of the support resources that are required to support the system when fielded or deployed. The SSP will be evaluated as part of the LD during DT and tested and certified as appropriate during OT. To influence OT design plans, it is advisable that draft descriptions of the SSP be provided 18 months before the start of testing, followed by approved descriptions 14 months prior to test start.

(1) *Simulation support plan sufficiency.* The PM/PEO/MATDEV, in coordination with the system evaluator and testers, will ensure that the SSP is sufficient to permit evaluation of logistic supportability issues in the TEMP. The SSP does not include those logistic support resources and services required by the tester to sustain the continuity of tests and demonstrations (for example, test site facilities and administrative support vehicle available at the test activity).

(2) *Simulation support plan delivery.* A complete SSP will be delivered to the test activity at least 30 days prior to test training initiation. When the SSP includes items available in the Army inventory, the responsible PM/PEO/MATDEV will ensure the on-site availability of such items. Upon receipt, test activities will inventory the SSP and report shortages that will have a significant impact on the planned test to the independent evaluators or assessors, and the logistician at least 25 days prior to scheduled test training initiation. If the system evaluator determines that SSP shortages exist that prevent the adequate evaluation of any supportability-related issues, test start will be suspended until the complete SSP is available, or the materiel proponent obtains a waiver. The ATIRS will be used for reporting the SSP inventory.

(a) Draft system support package components list delivery. The PM/PEO/MATDEV will ensure a draft system support package components list (SSPCL) is developed for any other test (developmental or operational) with critical supportability issues. The PM or MATDEV will furnish the draft SSPCL to the ILSMT or T&E WIPT members 90 days prior to test. They will review and identify SSP components required for each test in sufficient time for the PM, PEO, or MATDEV to acquire and deliver the SSP.

(b) Final system support package components list delivery. At least 60 days prior to the test training initiation, the PEO, PM, or MATDEV will provide two copies (or as otherwise specified) of the final SSPCL to the developmental and operational testers, system evaluator, logistician, CBTDEV, and any other interested activities.

6–58. New equipment training test support package

Based on the NET Program and with input from the TNGDEV, the PM, PEO, or MATDEV prepares, as appropriate, a NET TSP. It provides an equipment-specific training program for the TNGDEV or subject matter expert (instructor and key personnel) to develop a training program to train troops who will be used in a specific test. The NET TSP

contains a combination of equipment-specific documents, training aids, training devices, training simulators, programs of instruction (POIs), and lesson plans.

a. The NET TSP includes all training material required to train operators and maintainers on system peculiar tasks. The SSP should support the NET TSP and should be developed together with the NET TSP. Preparation of the NET TSP includes any contractor-developed training to be provided in support of OT. The NET TSP consists of the following sections: title of system, training aids (for example, transparencies, 35mm slides, student handouts, and blackboard), POI and lesson plans (draft or final), TMs (draft, commercial, or other), points of contact (support agency's point of contact name and telephone number required for initial coordination), remarks reflecting clarification of the above items (for example, time schedules, support package components, and additional support required to be placed in the system for test sustainment), and maintenance (including all maintenance charts and literature).

b. The PM, PEO, or MATDEV will program, budget, and fund the preparation and execution of the NET TSP. This includes, but is not limited to, training courses, and travel and per diem for instructor and key personnel training (IKPT). The NET TSP should be planned, developed, and executed in coordination with the trainer and concurrently with the SSP.

c. The TNGDEV or training proponent should use the NET TSP to develop the training TSP used by OT participants in support of OT execution. The developmental tester should use it in support of all DTs during the development process.

d. For non-tactical C4/IT systems, the NET TSP, if developed, should address both system hardware and software and be provided with the system to the FP for support of the planned testing assessments.

e. Milestones for providing NET TSP will be identified by the testers in either the TEMP or the OTP supporting the TSARC.

(1) The NET TSP should be provided to the developmental tester no later than 60 days prior to DT start. The milestone for delivery of the NET TSP to the developmental tester should be shown in the TEMP.

(2) The NET TSP should be provided no later than 180 days prior to start of training for an IOT. For NDI, the NET TSP should be provided no later than 60 days prior to start of training for the IOT. For EUT, LUT, and FOT, the NET TSP should be provided no later than 90 days prior to test start.

(3) To provide the best training possible, the system contractor may be allowed to train instructors as close to the start of training for start of IOT and FOT as feasible for knowledge retention purposes. Delivery of the NET TSP must still be timely to support delivery of the training TSP 60 days prior to start of training for IOT and FOT. Training aids, to include vehicles, should be provided to instructors as early as possible prior to the training test start date to train test players. The 180-day lead time cited in paragraph 6–58*e*(2) above is applicable for system contractor training. However, for NDI with more compressed milestone schedules, contractor training for the instructors may occur closer to start of the IOT. To ensure adequate planning, the PEO, PM, or MATDEV should notify the available agencies as the acquisition strategy is developed and establish mutually satisfactory milestone goals.

(4) The NET TSP should be provided to the TNGDEV as a package after completion of IKPT, which should be scheduled for completion 180 days prior (60 days when required for NDI) to the start of test player training in support of an IOT for a FRP DR.

(5) Deliveries of the NET TSP should be met even though the PEO, PM, or MATDEV may use contractor support to develop the NET TSP.

6–59. Doctrinal and organizational test support package

The D&O TSP can be prepared in support of both materiel systems development and C4I/IT systems development. The D&O TSP, provided by the CBTDEV, is used to expand, update, and add specificity to the information in the MNS and ORD documents to support planned operational tests required to support a scheduled DR milestone.

a. The D&O TSP will mature as the system and its requirements mature. Early in the system's life cycle, the content will be less specifically defined and subject to rapid changes as different concepts and techniques of employment and support are identified and accepted. As additional knowledge about the system and its capability increases, the more mature the D&O TSP becomes. As much information as possible should be provided to ensure support of operational test objectives as determined by the CBTDEV.

b. A D&O TSP typically supports the conduct of a LUT, IOT, and FOT. A D&O TSP may also be necessary in support of CEP, FDT/E, and EUT (as determined by the CBTDEV, operational tester, and system evaluator), but content will vary based on test or experiment requirements. The D&O TSP should be updated before each major test during a system's development.

c. The D&O TSP should be thought of as a transfer of approved system acquisition documents (for example, OMS/MP) or draft new or changes to operations documents (for example, field manuals (FMs)). Therefore, the

majority of the package should be filled by references to approved documents or attachments of draft documents (for example, draft FM change pages).

d. The D&O TSP consists of the following sections: references, means of employment, organization, logistics concepts, OMS/MP, test setting, and coordination. A suggested format for preparation of a D&O TSP is shown in figure 6–8. A majority of the details should be satisfied by references or attachments. When references are very large, specific pages/chapters should be identified to ensure appropriate use by the operational tester. A short paragraph should be provided for each item to help focus the tester to pertinent information.

1. **Title Page (type of test, system, and date).**
2. **References.** [1/]
3. **Means of Employment.** [2/]
   a. Field Manuals (FMs).
   b. Field Circulars (FCs).
   c. Training Circulars (TCS).
   d. Soldiers Manuals (SMs).
   e. Operators Manuals.
   f. Tactical Unit Standing Operating Procedures (TAC SOP).
   g. Communications-Electronic Operating Instructions (CEOI).
   h. Equipment Storage Plans (Load lists).
4. **Organization.** [3/]
   a. Basis of Issue Plan (BOIP).
   b. Qualitative and Quantitative Personnel Requirements Information (QQPRI).
   c. Organization Plan.
      (1) Introduction.
      (2) System Description.
      (3) Organizational Concept (Unit).
      (4) Operating Procedures.
5. **Logistics Concept.** [4/]
   a. Purpose.
   b. Source.
   c. Description.
   d. Supply.
   e. Transportation.
   f. Maintenance.
   g. Military Occupational Specialty by level of maintenance.
   h. Special tools and test equipment.
6. **Operational Mode Summary/Mission Profiles.** [5/]
7. **Test Setting.** [6/]
8. **Coordination.** [7/]

Footnotes:

[1/] References. The draft or approved MNS or ORD may be referenced or attached and all other documents supporting the D&O TSP appropriately referenced.

[2/] Means of Employment. This paragraph describes how the system will be employed and supported. It includes or references documents that describe the doctrine, tactics, techniques, logistical concepts and means of employment for the tested system, including a statement on new or revised versus current doctrine. The package should include sufficient detail to permit realistic system employment for conduct of the specified type test. It is used to guide the development of the SEP and to govern user actions during test. Also, when appropriate, related documents for the new system or equipment as well as support equipment should be shown as well as references or page changes to FMs, Field Circulars (FCs), Training Circulars (TCs), and operators manuals.

[3/] Organization. This element defines Military Occupational Specialty requirements, basis of issue, unit structure, organizational concept, operating concept, and lines of command or coordination for units employing the tested system. It is used in test planning to structure player units. When new Military Occupational Specialties are required, the specific duties of each Military Occupational Specialty level must be included in the D&O TSP. See AR 611-1, 30 Sep 97, regarding information for the development of this section. References to Basis of Issue Plan (BOIP), Quantitative and Qualitative Personnel Requirements Information (QQPRI), and Table of Organization and Equipment (TOE) apply.

Figure 6–8. Suggested format for a doctrinal and organizational test support package

[4/] Logistics Concepts. This paragraph describes the concept for planned supply, transportation, and maintenance procedures and methods for supporting the proposed or actual test system when fielded. If interim contractor support is planned in any form during initial fielding, then so state since laws govern system contractor or affiliates participation in IOT. References or draft change pages to appropriate FM apply. The concept will--

- Describe supply concepts envisioned for class I through X supply items and outline procedures for class IX repair parts availability for the system prescribed load list (PLL) including maintenance records, PLL records, requests for class IX items, and level of maintenance.
- Describe what supply and maintenance including repair parts and special tools will be provided to support testing.
- State system transportation procedures for rail, highway, marine and air movement with emphasis on new or changed requirements.
- State the Military Occupational Specialty and duty title for each required level of maintenance.
- Describe special tools and test equipment required to operate and maintain the system.
- Describe each level of maintenance responsibility during the test, that is, military personnel, Department of Army civilian employees or contractor personnel.
- Describe warranty procedures to be used to ensure maintenance conformity.
- Include coordination annexes listing the agencies through which the logistics concept was staffed and showing their comments. The logistics concept should be compatible with concepts, policies, and system support stated in AR 700-127 and AR 750-1. This section of the D&O TSP excludes the SSP by the PEO/PM/MATDEV but it should be compatible with the SSP.

[5/] Operational Mode Summary/Mission Profile (OMS/MP). This section presents a description of the anticipated mix of ways the new equipment will carry out its operational role. It includes the operational events and environment the equipment experiences from beginning to end of a specific mission laid out in a time-phased approach. Additionally, as required to satisfy the purpose of test, a set of operational mission profiles (that is, attack, defense) should be shown. This section is prepared by the CBTDEV or FP in coordination with the operational tester, to support the operational requirement. Details that should also be included or discussed for non-tactical C4/IT systems are workload, environment, mobilization, continuity of operations, data loss, and system peculiar events.

[6/] Test Setting. This paragraph should describe total environment (that is, tactical, threat, terrain, weather, and logistical support) under which the system is to be examined. The test setting defines the interactions among threat, friendly actions, and the environment (or some specific geographic location) and establishes a scenario that subjects the system under test in the context of its total environment, to include the next higher level system or organization. The test setting should be compatible with the Threat TSP. Also, the size of unit, OPFOR, and equivalent scale of operations should be stated. Reference any combat developer or standard scenario, whichever is applicable.

[7/] Coordination. This paragraph indicates the organizations that normally should be provided the D&O TSP for review and comment. The final D&O TSP should contain an enclosure or appendix, which details the results of the coordination. The combat developer or functional proponent should establish appropriate coordination requirements and all coordination schedules to support timely completion of the D&O TSP prior to approval. Information contained in the D&O TSP already approved should be annotated as such.

Figure 6–8. Suggested format for a doctrinal and organizational test support package—Continued

e. The CBTDEV is responsible for planning and development of the D&O TSP for each materiel system (or C4I/IT system) undergoing acquisition. The operational tester should assist CBTDEV in preparing the test setting (for example, scenarios and profiles) and concept of test employment. It is recommended that the Draft D&O TSP, to include the OMS/MP, be provided to the operational tester 27 months prior to the start of an IOT, a LUT, or FOT or as agreed

to by the T&E WIPT (or as agreed to between the CBTDEV and operational tester prior to the start of a CEP test, EUT, or FDT/E), and as shown in TSARC OTP. The CBTDEV must approve all D&O TSPs.

f. A checklist is provided at figure 6–9 for use by the preparer of the D&O TSP to ensure that basic contents of the TSP are addressed.

6–60. Threat test support package

Proponent CBTDEVs and MATDEVs provide threat support, including validation, to Army testing of new materiel and systems. (See app Y and AR 381–11.) The proponent threat support office will provide threat support by participating in test planning, preparing the threat TSP, providing training required by units portraying threat forces, and providing on-site monitoring of the threat portrayal prior to and during the test. This applies to all DTs, OTs, and other tests conducted in an operational setting.

a. Guidance regarding threat TSP content and format is contained in AR 381–11. Figure 6–10 provides a suggested preliminary package format for use as a guide during threat TSP preparation.

b. A threat TSP will be prepared when an operational threat is required for DT and OT of ACAT I and ACAT II systems, and other systems on the OSD T&E Oversight List. Specific testing requirements for a given system will be determined by the T&E WIPT. Determination of the requirement for an operationally realistic portrayal will be made by the T&E WIPT upon the recommendation of the evaluation organization based on the requirements of the TEMP.

c. The initial threat TSP (minus test-specific annexes) is developed after Milestone A by the CBTDEV or threat support organization to support future testing for a specific system or concept. This threat TSP is derived from the STAR or STA. The initial threat TSP is more detailed than the STAR or STA and provides the threat scenarios to support a specific test and assesses the impacts of threat-related test limitations. To support DT requirements, the PEO, PM, or MATDEV proponent (threat support organization or office) will expand and tailor the initial threat TSP for each test in which threat force operations are to be portrayed realistically. For OT, the CBTDEV or threat support activity will expand and tailor the initial threat TSP for each OT requiring a realistic threat portrayal.

d. The final threat TSP includes an update of the initial threat TSP plus a section of several appendices that are developed on an iterative basis to support specific tests approved by the TEMP. The appendices become part of the threat TSP and must be completed before final threat TSP approval can be granted.

e. As a member of the T&E WIPT for ACAT I systems, ACAT II systems, and OSD T&E oversight systems, the DA TISO advises threat representatives from the CBTDEV and MATDEV of tests scheduled and the anticipated threat support the requirements at the initial threat coordination group (TCG) meeting. TRADOC threat managers and AMC foreign intelligence officers serve as the principal TIs for OTs and DTs, respectively.

f. Threat TSPs for ACAT III systems not on the OSD T&E Oversight List will be provided by the CBTDEV or MATDEV, as appropriate, when threat portrayal is required by the T&E WIPT for a DT or OT.

g. When approved, the threat TSP describes the threat to be used for planning and developing the test and portrayed during test execution. An approved threat TSP, however, does not ensure that test threat portrayal is valid. Two separate approval actions are required, one for the threat TSP and one for the threat portrayal during the test. The approved threat is included in the approved T&E plan prior to execution of test.

h. See AR 381–11 for additional procedural and process guidance for threat TSPs.

6–61. Training test support package

The training TSP is provided to the test agency by the proponent developers of the new system. A training TSP is assembled by the proponent TNGDEV for each affected operator and maintainer military occupational specialty. Where there are system cross proponent responsibilities, the proponent for the requirement will assemble training materials for supporting Military Occupational Specialty. The lead proponent will consolidate the package and ensure it does not contain conflicting requirements. The training TSP contains information used by the trainer to train test players and for the tester's use in evaluating training on a new materiel system. It focuses on the performance of specific individual and collective tasks during OT of a system. The training TSP package should be updated prior to each EUT, LUT, IOT, and FOT during a system's development, or as required by the TEMP or OTP. Training TSP for non-tactical C4/IT and space systems should be tailored to the skills and abilities of the target audience scheduled to use the system. If there is no specified Military Occupational Specialty to use the information system, training should be addressed and the users described.

CHECKLIST FOR DOCTRINAL AND ORGANIZATIONAL TEST SUPPORT PACKAGE (D&O TSP)

1. Following is a list of items to consider during preparation and review of D&O TSP:
   a. References and title page. Administrative information and ORD/TSARC references (current and available).
   b. Means of Employment.
      (1) Does the D&O TSP provide a complete, current listing of the doctrinal materiel that will be required for the new system at the unit level (for example, FMs, FCs, TCs, SMs, operators manuals (may be included in the SSP), TAC SOPs, CEOIs, and load plans?
      (2) Does the D&O TSP provide a listing of the doctrinal material used at staff levels above the operating unit that must be changed or augmented to support fielding of the system? Interoperability?
      (3) Are drafts of, or changes to the listed or referenced documents included in the D&O TSP?
      (4) Is the draft documentation such that it addresses system employment and permits development of the SEP, EDP, DTP and other T&E planning documents (for example, TEMP and COIC)?
      (5) Are dates for delivery of the Tactical SOP, communication/electronic, and loading instructions and plans established?
      (6) Does the scope state the tactical scenario?
   c. Organization.
      (1) Are draft or final TOEs for units employing the system up to battalion level or equivalent included? BOIP, QQPRI referenced?
      (2) Does the D&O TSP include a detailed description of the operational concept for employing the system in combat to include lines of communication and coordination through division level?
      (3) Does the D&O TSP describe each of the system employment options (that is, direct support, general support, and attachment)?
      (4) Are the operating procedures for each option described in detail?
      (5) Are the lines of C3 for the system clearly delineated?
      (6) Are the degraded mode(s) of operation described in detail?
      (7) Are the various communications options (for example, wire, radio (voice, digital data, and secure), and facsimile.) described?
      (8) Are related operational and organizational concepts included in the D&O TSP? This applies when the system under development/test is used in conjunction with or to employ other systems. An example of a system requiring special treatment is the Fire Support Team Vehicle (FISTV), which in addition to its usual field artillery missions may be required to employ Hellfire missiles, U.S. Air Force laser guided, and conventional weapons and other systems. The D&O TSP should include the employment concepts for each such related system.
      (9) Are Military Occupational Specialties discussed?
   d. Logistics Concept.
      (1) Is the logistics concept for the system through the direct support level incorporated into draft FMs and support documents?
      (2) Is the logistics concept shown in FM (draft/final)?
      (3) Is the logistics concept detailed enough so that IOT and FOT can assess supportability through the direct support level?
      (4) Are all major logistical areas included (for example, supply, maintenance, and transportation).
      (5) Does the logistics concept include procedures for use of operational readiness floats (ORF)?
      (6) Type of support stated (troop, contract)?
      (7) Are there environmental impacts (for example, manufacturing, supply, maintenance, repair, and disposal actions)?

Figure 6–9. Doctrinal and organizational test support package checklist

e. Operational Mode Summary/Mission Profile.
(1) Has the OMS/MP been expanded or updated since the last operational test or publication of the ORD?
(2) Does the OMS/MP describe the events and frequency of occurrence and duration events in attack, defense, exploitation and retrograde operations? State alternate missions?
(3) Does the OMS/MP state the frequency and duration of responses to threat use of countermeasure such electronic warfare or radio electronic combat, obscurants, and NBC weapons?

f. Test Setting.
(1) Does the setting detail friendly and threat force actions down to the unit level?
(2) Are the probable areas of employment for the proposed system stated?
(3) Does the setting state the primary areas of employment for the proposed system?
(4) Is the approved scenario on which the test setting is based referenced? (Include sequence number and date of the scenario).
(5) Does the setting state or relate to a standard scenario and threat support package?
(6) Does the test setting identify the type force structure for the proposed system?

2. After finalizing contents, ensure that adequate coordination is accomplished.

Figure 6–9. Doctrinal and organizational test support package checklist—Continued

1. **Title page.** (Preparing agency, information cutoff date, U.S. system project office, and the MACOM or DA validation date).
2. **Tables of contents and illustrations.**
3. **Section I Background Information.**
   a. Description of system, organization or concept to be tested.
   b. Type of test.
   c. Evaluating agency.
   d. Test organization.
   e. TRADOC proponent school.
   f. Test dates.
   g. Test location.
   h. Simulated location (for example, central Europe).
   i. IOC of system being tested.
   j. Threat year.
4. **Section II Critical Operational Issues and Criteria/Additional Issues/Measures.**
5. **Section III Threat.**
   a. Specific threat systems and units/organizations.
   b. Threat tactics, doctrine, techniques, procedures and flight profiles, as appropriate.
   c. Threat countermeasures.
6. **Section IV Test Specific Appendices.**
   a. Appendix A: Test concept (Draft of SEP).
   b. Appendix B: Scenario.
   c. Appendix C: Description of trials/test runs/vignettes.
   d. Appendix D: Fire/target matrix.
   e. Appendix E: Targets, threat simulators, and surrogates.
   f. Appendix F: Limitations.
   g. Appendix G: Threat force training plan.

Figure 6–10. Suggested format for a threat test support package

a. Training TSPs usually consist of an initial submission and a final submission. The training TSP items identified below will be submitted for approval to TRADOC or MACOMs assigned responsibility for non-TRADOC systems.

(1) The initial training TSP contains the items listed below.

(a) STRAP. The STRAP should be approved by TRADOC prior to including it in the training TSP. Approval of the training TSP should not be construed as approval of the STRAP.

(b) Test training certification plan. The plan outlines and describes the method and procedures for evaluating and certifying individual and collective pre-test training. Specifically, it describes the who, where, and how training is certified.

(c) Training data requirements. Data requirements and milestones should be identified.

(2) The final training TSP contains the items listed below.

(a) Training schedule.

(b) POI for each military occupational specialty/specialty skill identifier affected.

(c) The Army external evaluation/mission training plan or changes to.

(d) List of training devices, embedded training components, and simulators.

(e) Target audience description.

(f) Soldier training publications or changes.

(g) Crew drills.

(h) Lesson plans.

(i) Ammunition, targets, and ranges required for training.

(j) Critical military occupational specialty task list.

(k) FMs or changes to FMs.

b. The proponent TNGDEV develops, coordinates, and provides the training TSP to the test agency. Logistics oriented schools and non-proponent schools that manage military occupational specialties involved with the new system develop training TSP input (for example, POI; Lesson plans; STRAP changes; training data requirements; external evaluation/mission training plan changes; target audience descriptions; crew drills; ammunition; targets and ranges required for training; and critical task list) to the lead proponent. This is in addition to the NET TSP provided by the MATDEV. All training TSP input must be provided in sufficient time from responsible agencies to the TNGDEV according to the following initial and final submission training TSP paragraphs, below, to allow the training TSP to be submitted on time to the tester. When required, a training TSP for an information system will be prepared as specified by the training proponent for the information system under development. The training TSP may provide or make reference to supporting documentation to the TSP. Attachments depend on availability of referenced documents.

(1) *Initial submission.* The initial training TSP consists of the draft STRAP or training data requirements, and the certification plan. It provides the test agency with the training concept for the system, the training issues upon which the trainer requires data, and the method for training test players. The initial submission is due to the test agency from Test (T) start minus (−) T–18 months, or as specified in the OTP.

(2) *Final submission.* The training TSP is prepared following IKPT and receipt of the NET TSP. It should be available 60 days prior to the commencement of test player training and the OTRR 2.

(3) *Functions.*

(a) The TNGDEV or proponent—

1. Provides guidance on preparation, coordination, approval, and distribution of the training TSP.
2. Serves as approving authority for all STRAPs and training TSPs.
3. Serves as the TNGDEV policy element for the STRAP and the training TSP.
4. Prepares initial and final training TSPs in coordination with supporting schools.
5. Forwards approved copies of initial and final training TSPs to the tester.

(b) The operational T&E activity.

1. Reviews the draft training TSP and provides comments to proponents.
2. Ensures the training TSP is included as part of the SEP development process.
3. Ensures all training is completed prior to start of test.

c. Figure 6–11 provides a checklist to use in preparing the TRAINING TSP.

CHECKLIST FOR TRAINING TEST SUPPORT PACKAGE
(Training TSP)

1. Initial Submission of the Training TSP.

a. Were development procedures followed for the STRAP?

b. Did the STRAP address:

(1) The system description?

(2) Assumptions?

(3) The training concept?

(4) The training device strategy?

(5) Significant training issues at risk?

c. Did the Test Training Certification Plan describe the method and procedures for evaluating and certifying individual and collective pre-test training? Specifically, did it describe the who, where, and how training is to be accomplished and the method of certification?

d. Were the STRAP and Test Training Certification Plan submitted within the time frame prescribed?

e. Did the Training Data Requirements provide training issues outlining the need for data on individual/collective performance, and technical manuals?

2. Final Submission.

a. Is final Training TSP submitted to HQ TRADOC at least 60 days prior to the test date?

b. Does the final Training TSP include:

(1) The training schedule?

(2) The POI for each Military Occupational Specialty/SSI affected?

(3) FMs/FM Changes References?

(4) The ARTEP/MTP or changes to the ARTEP/MTP?

(5) A list of training devices, embedded training components, and simulators?

(6) A target audience description?

(7) Soldier training publications or changes?

(8) Crew drills?

(9) Lessons Plans?

(10) A list of ammunition, targets, and ranges required for training?

(11) A critical task list?

c. Does the Training TSP include information from each Military Occupational Specialty proponent school affected?

d. Does the Training TSP lay out who is responsible for training those tasks taught in the institution and unit?

e. Does the Training TSP contain all of the material needed to train test players on operator and maintainer tasks?

f. Is field training necessary? Does it train operator crews to operate the system to its desired capability? Is night training appropriate?

g. Are TTPs taught to test players? Does it agree with the employment described in doctrinal manuals?

Figure 6–11. Training test support package checklist

h. Is there sufficient time built into the training schedule for the unit to become proficient with the system?
i. Will training devices be available to support test training?
j. How much ammunition is required to support training? Is it supportable?
k. Is the test player a "typical soldier" in his career field?

Figure 6–11. Training test support package checklist—Continued

Section V
System Safety Testing

6–62. Overview of system safety testing
One of the most important aspects of testing is verification of the elimination or control of safety and health hazards. Testing must include consideration of equipment and man-related failure. For example, are the failures related to mechanical, electrical, or chemical malfunctions or are the failures the result of man/item incompatibility, inadequacy of procedural guidance, or inappropriate or inadequate training, selection or orientation of personnel. (See app N.) There are no set rules or data lists established for safety requirements. However, because of similarities in categories of equipment, testers can establish operating procedures and sound engineering judgment can be applied. These initial areas are summarized at figure 6–12.

* Performance Requirements:
  - Man/item performance (speed, braking, range, and accuracy)
  - Levels of operator/maintainer training
  - Combat versus non-combat use

* Operational Conditions:
  - Location (land, sea, or air)
  - Climatic conditions (rain, cold, fog)
  - Types of Terrain (hills, desert, vegetation)
  - Time (daylight, night, continuous)
  - Command and control (communication)
  - Man-machine interface

* Hazard Considerations:
  - Noise level
  - Noxious fumes and gases
  - Mechanical hazards
  - Electrical hazards
  - NBC hazards
  - Fire hazards
  - Explosive hazards
  - Procedural hazards
  - Emergency procedures

Figure 6–12. Initial areas of safety consideration

6–63. Safety and developmental testing
To obtain the necessary data, the tester must, in most cases, observe test personnel performing the tasks required of an operator or maintainer. Until the safety envelope has been determined by operating the item near the maximum

safe limit, a thorough understanding of what the operator/maintainer has to do with, on, in, and around an item is unknown and critical hazards could exist. This is especially true of software controlled systems, where predictable and safe responses must result from computer failure, maintenance interlocks, power failures, and power-up tests.

a. A subtest entitled, "Safety and Health Hazards" is included in the test plan. Subtests for the analysis of safety parameters of systems and for developing safety release recommendations and other safety verification documents will reflect, as a minimum, safety test provisions of AR 385–10 and MIL–STD–882. A comprehensive subtest will be designed to establish the safety of the system including the following essential features:

(1) Preliminary examinations, review of the Safety Assessment Report, and limited tests necessary to certify through a safety release that the system is safe for further testing.

(2) Selected physical performance and reliability tests to verify that the system under test satisfies minimum design and construction requirements for safe field deployment.

(3) Systematic observations and analyses of the system throughout all phases of DT to identify and investigate any actual or potential hazards to personnel and equipment that may result from operation and maintenance of the system by representative users.

b. The test officer considers the following four areas of safety:

(1) Range safety ensures that test operations are conducted safely. The test officer ensures range safety with the support of safety personnel such as range control and the safety officer.

(2) Industrial rules governing vehicle safety, shop safety, and toxic substance safety primarily come from the test center safety office, OSHA Standards, and the HQDA and ATEC safety regulations and manuals. The test officer should be familiar with or obtain information on the rules governing the type of equipment being tested.

(3) Verification of equipment safety involves a compilation and analysis of all information provided to the test center and data generated by that center. The test officer will ensure that adequate testing is conducted to provide an accurate assessment of the safety of the test item. The safety evaluation subtests should be conducted to determine and verify that the item is safe. Exposure of test personnel will be held to an absolute minimum.

(4) The test officer should ensure testing is conducted within the guidelines of The Surgeon General/CHPPM and that Human Use Committee Review and statements of informed consent are obtained when required.

c. DT to provide safety data to support the safety release is front-loaded (that is, the test is designed so that safety data can be collected as early in the DT as possible). Specific safety tests are also performed on critical devices or components to determine the nature and extent of hazards presented by the materiel. Special attention is directed to—

(1) Verifying the adequacy of safety and warning devices and other measures employed to control hazards.

(2) Analyzing the adequacy of hazard warning labels on equipment and warnings, precautions, and control procedures in equipment publications.

d. Figure 6–13 reflects the minimum requirements regarding safety prior to initiation of Government DT.

e. The process to request a safety release from DTC is as follows Requests should be submitted as soon as the safety release requirement is known to DTC, ATTN: CSTE–DTC–TT–B (or to the appropriate test division, if known). Planning during the T&E WIPT process will provide DTC the opportunity to ensure the necessary testing is being done to provide data for the safety release. Include the following documents/information, if available:

(1) Safety assessment report.

(2) Health hazard assessment report.

(3) All test data available regarding the item requiring the safety release. If no current test data are available, any other information that can be used (for example, prior Government test data, contractor test data), with the emphasis on safety data.

(4) Environmental documentation.

(5) Training plans.

(6) Equipment publications.

(7) Mission scenario/MP.

(8) Test plan.

(9) Source of troops involved in OT.

(10) TEMP.

(11) When sufficient data are not available on which to base a safety release, it may be necessary that additional testing be done. In such cases, required testing will be performed by DTC and test costs will be paid by the MATDEV. The time required for issuing a safety release would increase accordingly. DTC will issue the safety release to the operational test activity with a copy furnished to TRADOC.

Safety Assessment Report (SAR) - must be thoroughly reviewed. The SAR should be available 60 days prior to test start.

Safety Standing Operating Procedures or Internal Operating Procedures (IOP) -for any hazardous operations, such as tests involving explosives, SOPs or IOPs must be developed and approved by the appropriate authority.

Precautions - are taken to protect personnel and equipment during tests.

Hazard Tracking List - is reviewed to identify the remedies that have been applied to correct previously identified hazards. Safety tests in developmental testing verify the adequacy of the remedy.

Environmental data - is reviewed to determine if the parameters are correct (for example, all systems are required to operate in the basic environment per AR 70-38). In addition, personnel have certain anthropometric characteristics that the system and the environment created by the system must take into consideration (for example, vibration created by operating the system must be below the "uncomfortable" range to prevent possible internal injury).

Human Use Committee - Review conducted for those tests performed by personnel who are not "testers by duty assignment" (for example, non-professional testers).

Independent Safety Assessment - prepared by the USASC and forwarded to the AAE assessing the risk of the residual hazards in a system prior to the MDR's.

Figure 6–13. Minimum safety requirements done to provide data for the safety release

6–64. Safety release

OT, including pretest system training, demonstrations, experiments, and DT involving Soldiers will not begin until the test agency, the trainer, and the commander who is providing the Soldiers have received a safety release. The safety release is developed at least 30 days prior to pretest training and at least 60 days prior to all types of OT and DT that expose Soldiers to training and testing activities involving the research, development, operation, maintenance, repair, or support of operational and training materiel. This requires that pertinent data (for example, results of safety testing, and hazard classification) be provided to the safety release authority in sufficient time to perform this testing or determine if additional testing is required.

a. Copies of the safety release are also issued to the system evaluator, CBTDEV, and PM. DTC does not provide the safety release for systems developed by USAMEDCOM.

b. The safety release indicates the system is safe for use and maintenance during the specified test by typical user troops and describes the specific hazards of the system based on test results, inspections, and system safety analyses. Operational limits and precautions are also included. The requirement for a safety release also applies to testing of new or innovative procedures (for example, doctrine and TTP) for the use of materiel that has been type classified. Safety releases are not required for use of standard equipment in the normal prescribed manner.

c. A conditional safety release is issued when further safety data are pending or operational restrictions are required that restrict certain aspects of the test (for example, a restriction on range fan area until all range safety tests are completed).

d. A limited safety release is issued on one particular system (that is, prototype, model, modification, and software revision) or for one particular test.

e. The tester uses the information contained in the safety release to integrate safety into test controls and procedures and to determine if the test objectives can be met within these limits.

f. When unusual health hazards exist, The Surgeon General reviews or participates in preparation of safety releases to ensure safety of user troops during OT.

g. The safety release format is reflected in AR 385–10.

6–65. Safety confirmation

The safety confirmation is prepared by ATEC's DTC and appended to the SER. It is also provided to the PM, AMC Safety Office, and the U.S. Army Safety Center. It indicates if specific safety requirements are met and includes a risk assessment for those hazards not adequately controlled. It lists any technical or operational limitations or precautions as well as highlighting any safety problems that require further investigation and testing. Earlier safety confirmations may be provided at major acquisition milestone junctures. See appendix N for additional information.

Section VI

Interoperability and Certification Testing

6–66. Overview of interoperability and certification testing

DoDD 5000.01 and DoDI 8330.01 require that all acquired systems be interoperable with other U.S. and allied systems, as defined in the requirements and interoperability documents. Interoperability issues are considered during development of the T&E strategy. USMTF, TDL provide standardized messaging capabilities and enable seamless interoperability within the infosphere.

a. The TEMP includes at least one CTP and one operational effectiveness issue for evaluation of interoperability. (See chap 3.)

b. The system evaluator reviews the major documents that define the system's interoperability environment and monitors the major events that produce information on compatibility and interoperability. The following are the potential sources of interoperability information:

(1) Army Battlefield Interface Concept (ABIC) is produced by the CBTDEV (usually TRADOC) and identifies the intra-Army, inter-Service, and NATO systems architecture and associated interfaces. It serves as the primary document that defines the systems with which a developing system is expected to operate.

(2) IERs are developed by the CBTDEV, documented in the C4ISP, and provide quantifiable data to characterize each required information exchange.

(3) Technical interface design plans are the technical design documents for each interface. They are developed by the MATDEV and provide the technical interface parameters, message formats, message content, and implementation requirements.

(4) Interface specifications are developed by the MATDEV and provide detailed technical engineering information on system interfaces.

(5) Interface control documents are developed by the MATDEV and describe the physical and electrical connections, voltage, and current requirements, and provide interface control drawings. Interface control documents are a source of data for operational evaluation.

(6) Interface operating procedures are developed by the MATDEV and describe the man-machine interfaces and standardized operating procedures for multiple interfacing systems. For NATO system interfaces, interoperability is guided by standardization agreements (STANAGs).

(7) Operator and user handbooks are developed in parallel with the system by the MATDEV in coordination with the user, and provide SOPs and user procedures relevant to the operation of the system.

c. The ORD, C4ISP, and ABIC enable the system evaluator to identify the interfacing systems and the systems for which interface is a concern. The ORD and IERs are used to identify the factors and conditions that have the potential to impact the system's interoperability requirements. Compatibility issues are identified by the system evaluator based on review of the IERs and the description of the environment from the ORD.

6–67. Joint/Combined/North Atlantic Treaty Organization certification overview

All national security systems and information technology (IT) systems, regardless of Milestone A, B, and/or C, must be tested and testing results certified by DISA, JITC. Joint Certification Testing can be performed in conjunction with other testing with the U.S. Army CECOM SEC APTU and the AMCOM SED aviation, air, and missile defense participating systems whenever possible to conserve resources. Interoperability evaluation and testing is conducted throughout the life cycle of National Security Systems and C4I/IT systems and interfaces but should be achieved as early as practical to support scheduled procurement decisions.

6–68. U.S. Army Communications-Electronics Command Software Engineering Center Army Participating Test Unit Coordinator's role in the Joint/Combined/North Atlantic Treaty Organization certification testing requirements

Joint and DoD directives have directed that "all C4I systems developed for use by U.S. forces are considered to be for joint use." The Joint Chiefs of Staff have published MIL–STD–6011, MIL–STD–6016, MIL–STD–6040, Joint Variable Message Text Format Technical Interface Design Plan Test Edition (TE), and NATO STANAG 5516 that are designed to ensure systems meet end users' information exchange needs as well as their interoperability requirements. The FRP DR now depends on successful joint interoperability certification. Joint/Combined/NATO certification requirement policies are stated in the following documents:

a. DoDI 8330.01.
b. JITC PLAN 3006.
c. AR 73–1.
d. CECOM Regulation 10–1.
e. STANAG 5516.

6–69. North Atlantic Treaty Organization interoperability testing

NATO interoperability testing is required as part of the NATO policy for C3I. Army participation in NATO interoperability testing is coordinated through the APTU. Testing methodology is defined in the NATO Interoperability Framework, which delegates its North Atlantic Treaty Organization Consultation, Command and Control Interoperability Environment (NIE) testing to the North Atlantic Treaty Organization Consultation, Command and Control Interoperability Environment Testing Working Group (NIETWG). The North Atlantic Treaty Organization Interoperability Environment Testing Infrastructure (NIETI) coordinates the NATO Interoperability Testing Program. Within the NIETWG, the Tactical Data Link Interoperability Testing Syndicate (TDLITS) is responsible for the testing of TDLs. The program of work for the TDLITS will be coordinated by the NIETI, once this organization is fully established. See figure 6–14.

CHECKLIST FOR NATO TESTING

Following is a list of items, which must be in place for systems participating in NATO testing:

1. The TDLITS will review applicable system documentation, which includes:
   a. Requirements documents (that is, MNS and ORD, to include IERs)
   b. Concept of Operations (CONOPS)
   c. Standard NATO Agreements (STANAGs)
   d. System Interface Design Documents (SIDDs)
   e. Allied Data Publications (ADatP)

2. Prior to testing, the TDLITS will review previous NIETI or other nation's test results to include all NATO nations and organizations, agencies one-on-one test results.

3. Test types (as specified by the Test Director (TD)) include both NIE Standards and Implementation Testing. In addition to these test types, there are four levels of testing, which include paper-based, rig-based, live, and simulation.

4. Test Cycle
   a. Objectives and procedures - The TDLITS establishes the test objectives and works with the TD and participating nations to develop test procedures or serials that meet specific test requirements.
   b. Pre-test coordination - All participants review and approve the NTDLIOT test procedures. Pre-test reviews are conducted two weeks prior to testing, and include a last minute review of the test procedures and overall test conduct.
   c. Control - The NATO Tactical Data Link Interoperability Test TD (NTDLIOT) controls test conduct in co-ordination with the National TD (NTD). The test is conducted by exchanging messages based on test events and stimulating sensors to test conformance and confirming interoperability in accordance with applicable STANAGs and approved Data Link Change Proposals (DLCPs).
   d. Monitoring - During the TDL test execution, the systems and the NTDLIOT TD monitors, records and extracts test data to support post test analysis.
   e. Test integrity - Participating systems should not be altered during a test without explicit concurrence of the NTDLIOT TD and the nation's TD.
   f. Multi-link and special requirements - If nations are capable of operating simultaneously on multiple data links (for example, to perform concurrent operations), providing data translations from one message to another standard to another (such as forwarding from Link 11 to Link 16), these capabilities will be tested during NTDLIOTs, if resources are available to do so.
   g. Test Analysis - Post test procedures (Preliminary Trouble Reports, Trouble Reports, ARP conduct and Test Reporting) shall be in accordance with the NATO C3 Interoperability Environment Testing Concept. The NATDLIOT TD is responsible for preparing both the final test procedure and the test report. The NATDLIOT TD will also collect all relevant recorded data and test results and will transfer these together with the test procedures to appropriate media for storage and retrieval purposes.

Figure 6–14. Checklist for North Atlantic Treaty Organization testing

6–70. Tactical data links testing process

a. Army participating test unit coordinator. CECOM SEC is the APTUC. In this role, the SEC represents the Army at all the Joint message standards/certification forums to include the Joint Configuration Control Board (CCB) and other Joint Working Group Meetings. SEC APTUC is the focal point for configuration management of all the joint message standards and joint certification testing. U.S. Army PMs/PEOs coordinate through the AMCOM SED, as appropriate, to CECOM SEC APTUC and JITC for systems to be certified in joint/combined/NATO areas. A master test schedule is developed so that the PMs/PEOs will have a scheduled place for their system early in program development. The certification process is divided into three phases—

(1) Pre-test.

(a) Assures Army participation in review and submission of inputs to joint interoperability test documents.

(b) Coordinates the dissemination of test documentation.

(2) Test.

(a) Supports the joint test by providing technical and engineering support.

(b) Analyzes, evaluates and records data produced during joint testing for Army systems.

(3) Post test.

(a) Writes preliminary trouble reports as a result of test analysis and evaluation. Prepares preliminary trouble reports for transmission to the JITC and other participating Army units.

(b) Attends Joint Analysis Review Panel (JARP) and serves as the Army's spokesperson or voting member. Also provides technical support to the Army Systems.

(c) Assigns trouble reports to all valid problems and assign criticality category per table 6–6.

b. Problem probability assignment. All trouble reports will be assigned a probability of occurrence (A through E) by the JARP based upon criteria presented in table 6–7.

c. Trouble report risk assessment. Trouble report risk assessment will be made by the JARP based on the identified severity and probability of occurrence. Table 6–8 presents the possible combinations of severity and probability that equate to a resultant risk assessment. Based on JARP concurrence, the JITC will assign a high, medium, or low risk assessment to trouble reports prior to delivery to sites/programs for further adjudication.

Table 6–6
Severity and joint task force impact

Category	Definition	Joint Task Force (JTF) Impact
1	Prevents the operator's accomplishment of an operational or mission essential function or which jeopardizes personnel safety.	JTF operations or communications cannot be completed, or personnel safety jeopardized.
2	Adversely affects the accomplishment of an operational or mission essential function so as to degrade performance and for which no alternative "work-around" solution exists.	JTF operations or communications are severely degraded. No acceptable TTPs exist.
3	Adversely affects the accomplishments of an operational or mission essential function and for which there is a "reasonable" alternative work-around solution.	Problem has the potential to severely degrade JTF operations or communications, but operators consider TTP acceptable.
4	Operator inconvenience or annoyance	JTF operations or communications are slightly degraded but all ops may proceed.
5	All others.	JTF operations or communications are not impacted but enhancement is desirable.

Table 6–7
Probability of occurrence

Probability	Level	Probability description
Frequent	A	Likely to occur frequently, essentially equal to a probability of 1.
Probable	B	Will occur several times during a test event.
Occasional	C	Likely to occur sometime during a test event, essentially equal to a probability of 0.5.
Remote	D	Unlikely to occur during a test event, but possible.
Improbable	E	Extremely unlikely to occur, essentially equal to a probability of zero.

Table 6–8
Trouble report risk assessment—Continued

	Severity category				
Probability level	1	2	3	4	5
A - Frequent	I	I	II	II	III
B - Probable	I	I	II	II	III
C - Occasional	II	II	III	III	IV
D - Remote	II	II	III	IV	IV
E - Improbable	III	III	III	IV	IV

Notes.
I. Very high risk—Must resolve as soon as possible
II. High risk—Immediate resolution desirable
III. Manageable risk—Resolution can be delayed
IV. Low risk—Resolution not required

Section VII

Instrumentation, Targets, and Threat Simulators

6–71. Instrumentation, targets, and threat simulators requirements

Every test requires an element of ITTS. Acquisition of ITTS follows AR 70–1.

6–72. Instrumentation, targets, and threat simulators planning

Appendix Z discusses the planning of ITTS to meet T&E requirements. It outlines the relationships of key activities involved in planning, managing, and using ITTS in support of T&E. It also identifies key inventory and capability accounting systems, describes procedures for asset scheduling and use, and identifies existing Army major range and test facilities, major instrumentation, and test equipment. Appendix Z identifies assets by location, value, capability, and points of contacts to provide the test community with a readily available list of assets.

Appendix A

References

Section I

Required Publications

AR 70–1
Army Operation of the Adaptive Acquisition Framework (Cited in paras 1–1*a*, 2–2, 5–4*a*(1), 5–12*a*, 6–5, 6–5*a*, and 6–71.)

AR 73–1
Test and Evaluation Policy (Cited in the title page.)

DA Pam 70–3
Army Acquisition Procedures (Cited in paras 2–2, 5–5*c*, and 6–5 and app K.)

Section II

Related Publications

A related publication is a source of additional information. The user does not have to read a related publication to understand this pamphlet. Unless noted otherwise below, DoDDs and DoDIs are available at https://www.esd.whs.mil/DD/. IEEE standards are available at https://standards.ieee.org/. ISO/IEC publications are available at https://www.iso.org/.

AR 1–20
Legislative Liaison

AR 5–11
Management of Army Models and Simulations

AR 25–1
Army Information Technology

AR 25–2
Army Cybersecurity

AR 25–30
Army Publishing Program

AR 25–55
The Department of the Army Freedom of Information Act Program

AR 40–10
Health Hazard Assessment Program in Support of the Army Acquisition Process

AR 40–60
Army Medical Materiel Acquisition Policy

AR 70–25
Use of Volunteers as Subjects of Research

AR 70–38
Research, Development, Test and Evaluation of Materiel for Worldwide Use

AR 70–47
Engineering for Transportability Program

AR 70–62
Airworthiness of Aircraft Systems

AR 70–75
Survivability of Army Personnel and Materiel

AR 71–9
Warfighting Capabilities Determination

AR 350–1
Army Training and Leader Development

AR 350–38
Policies and Management for Training Aids, Devices, Simulators, and Simulations

AR 360–1
The Army Public Affairs Program

AR 380–5
Army Information Security Program

AR 380–381
Special Access Programs (SAPs) and Sensitive Activities

AR 381–10
The Conduct and Oversight of U.S. Army Intelligence Activities

AR 381–11
Intelligence Support to Capability Development

AR 385–10
The Army Safety and Occupational Health Program

AR 602–2
Human Systems Integration in the System Acquisition Process

AR 611–1
Military Occupational Classification Structure Development and Implementation

AR 700–127
Integrated Product Support

AR 702–7–1
Reporting of Product Quality Deficiencies Within the U.S. Army

AR 750–1
Army Materiel Maintenance Policy

AR 750–10
Army Modification Program

AR 750–43
Army Test, Measurement, and Diagnostic Equipment

AR 770–2
Materiel Fielding

AR 770–3
Type Classification and Materiel Release

Army Research and Acquisition Bulletin
O'Bryon, J.F., Live Fire Testing: Legislation and Its Impact, pp. 1–3, 1987.

CMU/SEI–87–TR–23
Carnegie Mellon University Software Engineering Institute Technical Report, A Method for Assessing the Software Engineering Capability of Contractors (Available at https://www.sei.cmu.edu/publications/.)

CMU/SEI–2002–TR–01, Version 1.1
CMMISM for Systems Engineering/Software Engineering/Integrated Product and Process Development/Supplier Sourcing Continuous Representation (CMMI–SE/SW/IPPD/SS, V1.1, Continuous) CMMI Product Development Team (Available at https://www.dtic.mil/).

CMU/SEI–2002–TR–010, Software Acquisition Capability Maturity Model® (SA–CMM®) Version 1.03
CMMISM for Systems Engineering/Software Engineering/Integrated Product and Process Development/Supplier Sourcing, Version 1.1, Continuous Representation (CMMI–SE/SW/IPPD/SS, V1.1, Continuous) CMMI Product Development Team (Available at https://www.dtic.mil/).

CMU/SEI–2002–TR–012
CMMISM for Systems Engineering/Software Engineering/Integrated Product and Process Development/Supplier sourcing Staged representation (CMMI–SE/SW/IPPD/SS, V1.1, Staged). (Available at https://www.dtic.mil/).

CTA 50–900
Clothing and Individual Equipment

CTA 50–970
Expendable/Durable Items

DA Pam 5–11
Verification, Validation, and Accreditation of Army Models and Simulations

DA Pam 700–127
Integrated Product Support Procedures

DA Pam 770–2
Procedures for Materiel Fielding

DA Pam 770–3
Type Classification and Materiel Release Procedures

Defense Acquisition Guidebook
(Available at https://aaf.dau.edu/guidebooks/.)

DoD 3235.1–H
Test and Evaluation of System Reliability, Availability, and Maintainability—A Primer

DoD 4245.7–M
Transition from Development to Production (Available at https://apps.dtic.mil/sti/tr/pdf/ada303209.pdf.)

DoD 5000.3–M–4
Joint Test and Evaluation Procedures Manual (Available at https://apps.dtic.mil/sti/citations/ada268035.)

DoDD 3200.11
Major Range and Test Facility Base (MRTFB)

DoDD 3405.1
Computer Programming Language Policy

DoDD 5000.01
The Defense Acquisition System

DoDD 5000.59
DoD Modeling and Simulation (M&S) Management

DoDI 5000.02
Operation of the Adaptive Acquisition Framework

DoDI 5000.61
DoD Modeling and Simulation (M&S) Verification, Validation, and Accreditation (VV&A)

DoDI 5010.41
Joint Test and Evaluation (JT&E) Program

DoDI 8330.01
Interoperability of Information Technology, Including National Security Systems

DoDI 8500.01
Cybersecurity

DoDI 8510.01
Risk Management Framework for DoD Systems

DoD–STD–1838
Common ADA Programming Support Environment (APSE) Interface Set (CAIS)

HQDA Army Guidelines
"Use of Modeling and Simulation (M&S) to Support Test and Evaluation (T&E)," 18 April 2000

IEEE Standard 730
Standard for Software Quality Assurance Processes

IEEE Standard 982.1
Standard Dictionary of Measures of the Software Aspects of Dependability

IEEE Standard 1008
Standard for Software Unit Testing

IEEE Standard 1012
Standard for System, Software, and Hardware Verification and Validation

IEEE Standard 1012a
Standard for Software Verification and Validation—Supplement to 1012–1998—Content

IEEE Standard 1028
Standard for Software Reviews

IEEE Standard 1058
Standard for Software Project Management Plans

IEEE Standard 1058.1
Standard for Software Project Management Plans

IEEE Standard 1061
Standard for Software Quality Metrics Methodology

IEEE Standard 1063
Standard for Software User Documentation

IEEE Standard 1362
Guide for Information Technology—System Definition—Concept of Operation Document

IEEE Standard 1540
Standard for Software Life Cycle Processes—Risk Management

ISO/IEC 9126–1
Software engineering—Product quality—Part 1: Quality model

ISO/IEC 12207
Information technology—Software Life Cycle Processes

ISO/IEC 14598–5
Information technology—Software product evaluation—Part 5: Process for evaluators

ISO/IEC 14756
Information technology—Measurement and rating of performance of computer-based software systems

ISO/IEC 15026
Information technology—System and software integrity levels

ISO/IEC/IEEE 29119–3
Software and systems engineering – Software testing – Test documentation

ISO/IEC TR 15271
Information technology—Guide for ISO/IEC 12207 (Software Life Cycle Processes)

ISO/IEC TR 15846
Information technology—Software life cycle processes—Configuration Management

ISO/IEC 15910
Information technology—Software user documentation process

ITOP 1–1–056
Software Testing (Available at https://vision.atc.army.mil/.)

Joint Interoperability Test Command Plan 3006
Joint Interoperability Test Plan (Available at https://jitc.fhu.disa.mil/index.aspx.)

MIL–HDBK–189C
Reliability Growth Management (Available at https://quicksearch.dla.mil/qssearch.aspx.)

MIL–HDBK–245E
Preparation of Statement of Work (SOW) (Available at https://quicksearch.dla.mil/qssearch.aspx.)

MIL–HDBK–881A
Work Breakdown Structures for Defense Materiel Items (Available at https://quicksearch.dla.mil/qssearch.aspx.)

MIL–STD–461G
Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment (Available at https://quicksearch.dla.mil/qssearch.aspx.)

MIL–STD–464D
Electromagnetic Environmental Effects Requirements for Systems (Available at https://quicksearch.dla.mil/qssearch.aspx.)

MIL–STD–810H
Environmental Engineering Considerations and Laboratory Tests (Available at https://quicksearch.dla.mil/qssearch.aspx.)

MIL–STD–882E
System Safety (Available at https://quicksearch.dla.mil/qssearch.aspx.)

MIL–STD–2169D
High-Altitude Electromagnetic Pulse (HEMP) Environment (Available at https://quicksearch.dla.mil/qssearch.aspx.)

MIL–STD–6011F
Tactical Digital Information Link (TADIL) 11/11B Message Standard (Available at https://quicksearch.dla.mil/qssearch.aspx.)

MIL–STD–6016G
Tactical Digital Information Link (TADIL) 16 Message Standard (Available at https://quicksearch.dla.mil/qssearch.aspx.)

MIL–STD–6040B
U.S. Message Text Format (USMTF) Description (Available at https://quicksearch.dla.mil/qssearch.aspx.)

RADC–TR–87–171, Volumes 1 and 2
Methodology for Software Reliability Prediction (Available at https://apps.dtic.mil/sti/tr/pdf/ada190018.pdf.)

Rules of the Road: A Guide for Leading Successful Integrated Product Teams
(Available at https://www.dau.edu/cop/pm/documents/rules-road-guide-leading-successful-integrated-product-teams.)

21 CFR 50
Protection of Human Subjects (Available at https://www.ecfr.gov/.)

21 CFR 56
Institutional Review Boards (Available at https://www.ecfr.gov/.)

21 CFR 312
Investigational New Drug Application (Available at https://www.ecfr.gov/.)

5 USC Chapter 10
Federal Advisory Committees (Available at https://uscode.house.gov/.)

10 USC 139
Director of Operational Test and Evaluation (Available at https://uscode.house.gov/.)

10 USC 4171
Operational test and evaluation of defense acquisition programs (Available at https://uscode.house.gov/.)

10 USC 4172
Major systems and munitions programs: survivability testing and lethality testing required before full-scale production (Available at https://uscode.house.gov/.)

Section III

Prescribed Forms

Unless otherwise indicated, DA forms are available on the Army Publishing Directorate website (https://armypubs.army.mil).

DA Form 7492
Test Incident Report (Prescribed in para V–2*b*.) (Available only in ATIRS at https://vision.atc.army.mil).

Section IV

Referenced Forms

This section contains no entries.

Appendix B

Test and Evaluation Master Plan Checklist

B–1. Test and Evaluation Master Plan 101 Brief

TEMA, in coordination with the TEMAC, provides additional guidance for the development and staffing of a TEMP on CD–ROM and the TEMA website at http://www.hqda.army.mil/tema. The TEMP 101 Brief is virtual in nature and as such provides links to previously approved (OSD/Army) portions of a TEMP that serve as examples and practical applications of the regulatory guidance.

B–2. Test and evaluation master plan checklist

This checklist (fig B–1) is intended as a guide to both TEMP developers and TEMP reviewers. The checklist, when properly used, should ensure that all necessary and appropriate requirements in the approved T&E strategy are adequately considered and efficiently address T&E and program execution.

PROGRAM: Tactical Unmanned Aerial Vehicle

CURRENT TEMP MS: TUAV-333-TEMP-v3.2 DATE OF REVIEW: 10 Jan 02

REVIEWED BY: MAJ Joseph Prime, PM TUAV

Cover Sheet
Does the page identify the necessary program information, date, version of the TEMP, and category of the program?

Approval Page
a. Does the page contain the necessary signatures for the acquisition category of the program?
b. Is a date at the top of the page?
c. Is there an update number if this is not an initial submission?
d. Is there a revision number if this version contains changes based on comments subsequent to T&E WIPT concurrence from HQDA and/or OSD on reviews?

T&E WIPT Coordination Sheet
Are there signature blocks for—
a. Program Manager?
b. Combat Developer?
c. System Evaluator (AST Chair)?
d. Developmental Tester?
e. Operational Tester?
f. Logistician?
g. Threat Integrator?
h. Survivability/Lethality Analyst?
i. E3/SM and/or JSC SME?
j. HQDA Staff
(1) ASA(ALT)?
(2) DCS, G-1?
(3) DCS, G-2?
(4) DCS, G-3?
(5) DCS, G-8?
(6) ASA(ALT) ILS?
(7) DUSA(OR)?
(8) CIO/G-6?
k. Others as required

Part I. System Introduction
a. Mission Description.
(1) Mission of the deployed system briefly described?
(2) Does the mission description agree with the MNS, CRD (if applicable), C4ISP, and/or ORD?
(3) Is the need defined in terms of mission, objectives, and general capabilities?
(4) Is the MNS referenced and listed in appendix A - Bibliography?
(5) Does the mission describe the operational and logistical environment envisioned for the system?

b. System Description.
(1) System design briefly described?
(2) Key features of both hardware and software and subsystems allow the system accomplishment of operational mission described?
(3) Interfaces/interoperability with existing or planned systems that are required for mission accomplishments described? Picture included?
(4) Are critical characteristics of the system or unique support concepts resulting in special test and evaluation requirements listed?
(5) System software, if used, described?

Figure B–1. Test and evaluation master plan checklist

(6) Are existing and/or planned systems of other DOD Components or allies for which interoperability with this system is required listed?
(7) Is intra-Army interoperability certification addressed?
(8) Has the description of the overall system included Mission Critical Computer Resources (MCCR) for software utilized by the system?
(9) Have key processors, software (including firmware) configuration items, system interfaces, internal and external message standards, and protocols been identified?
(10) Does the system description address equipment that contains (or will contain) electronic or electrical components?
(11) Does the system description address frequency spectrum dependent equipment?
(12) What are the technical risks for the program's development?
(13) What is the program's risk management approach for hardware and software?

c. System Threat Assessment.
(1) Is the system threat briefly described?
(2) Is the operational threat environment summarized from the STAR?
(3) Is the threat at IOC plus 10 years and the reactive threat listed?
(4) Is the STAR referenced in Annex A - Bibliography?

d. Measures of Effectiveness and Suitability.
(1) Are the critical operational effective, suitability, and survivability parameters and constraints summarized from the ORD?
(2) Is the ORD referenced and listed in Annex A - Bibliography
(3) Are thresholds and objectives expressed as values?

e. Critical Technical Parameters.
(1) Critical technical parameters that have been/will be evaluated during all phases of development listed in the matrix? (Include software maturity and performance metrics and technical interoperability.)
(2) Accompanying technical threshold listed next to each technical parameter?
(3) Are results from developmental test addressing a given parameter posted?

Part II. Integrated Test Program Summary

a. Integrated Test Program.
(1) Does integrated test program address these areas of interest:
(a) Milestones?
(b) Acquisition events?
(c) Contract awards and events?
(d) Product deliveries, to include test article availability and the schedule of major software releases?
(e) Developmental test?
(f) Live fire test and evaluation?
(g) Operational test?
(h) E3/SM
(2) Does the funding data correspond to programmatic forecasts & contain all categories of funding as described in AR 37-100-FY:
(a) MRTFB Reimbursable identified?
(b) RDTE identified?
(c) Procurement identified?

b. Management.
(1) T&E responsibilities of all participating organizations outlined?
(2) Is the T&E WIPT charter referenced in Annex A - Bibliography?
(3) Is a clear definition of LRIP and full-rate production provided?
(4) Is the date of the decision to proceed beyond LRIP provided?
(5) Have participating organizations responsible for software T&E been identified?

Figure B–1. Test and evaluation master plan checklist—Continued

(6) Are vulnerability and lethality Live Fire Test requirements and operational issues that cannot be addressed before proceeding beyond LRIP explanations provided?
(7) Are responsibilities for configuration management of test articles designated?
(8) Are responsibilities for establishing a HUC designated?
(9) Is the HUC determination that further review is not required documented here, and that document listed in Annex A - bibliography?
(10) Do the quantities required for DT and IOT&E correspond to those quantities designated in Part V?
(11) Have the proposed or approved performance exit criteria to be assessed at the next acquisition milestone been included?
(12) Are responsibilities for DITSCAP process and certification identified?
(13) Are the procedures and responsibilities for OT certification identified?

Part III. Developmental Test and Evaluation Outline

a. Developmental Test and Evaluation Overview.
(1) Explanation included of how planned DT will verify--
(a) Status of engineering design and development?
(b) Design risks have been minimized ?
(c) Achievement of technical performance?
(2) Identify any technology or software that has not demonstrated its contribution to system performance in relationship to the system risk assessment.

b. Readiness for IOT
(1) Are technologies identified which have not been demonstrated?
(2) Is the degree to which the system has stabilized been addressed?
(3) Has a discussion of the indicators that will be used to determine software status and evaluate progress toward software maturity in support of key decision points been identified?
(4) Are early developmental tests scheduled which will mitigate the technical risks identified in the Integrated Program Summary, Annex D?
(5) Is the Integrated Program Summary referenced in Annex A - Bibliography?
(6) Are developmental tests, which feed into operational tests or evaluations, identified?
(7) Is a Logistics Demonstration planned prior to the FRP IPR ?
(8) Are tests that validate supportability requirements (that is, TMs and support packages) identified?
(9) Is the test that will validate the program's requirements against the system specification identified?
(10) Has survivability/lethality testing been highlighted?
(11) Has applicable intra-Army interoperability certification been addressed?
(12) Are developmental test events that will be used to evaluate E3 vulnerabilities identified?
(13) Has DT performance exit criteria for OT been met?

c. Future Developmental Test and Evaluation.
(1) Are developmental tests designated which will demonstrate test item safety; supportability (that is, verify and validate technical manuals and support packages) and that specifications are met?
(2) Are survivability/lethality testing as well as those tests addressing conventional weapon effects, E3, ECM, ECCM, initial nuclear weapon effects, advanced technology survivability, and NBC contamination identified?
(3) Are test plans and strategies to validate the manufacturing process identified?
(4) Are the following areas addressed:
(a) RAM?
(b) Survivability?
(c) Electromagnetic Capability?
(d) Human Factors?
(e) System Safety?
(f) Health Hazard?
(g) Environment?
(h) Integrated Logistical Support?
(5) Is each test or phase presented in the following format: Configuration Description; DT&E Objectives; DT&E Events, Scope, Basic Scenario, and Limitations?

Figure B–1. Test and evaluation master plan checklist—Continued

(6) Are the differences between the system to be tested and objective system stated for each test (if necessary)?
(7) Are the resources required for each test identified in Part V?
(8) Are test and evaluation related exit criteria identified in the Acquisition Decision Memorandum (ADM) addressed?
(9) Are test limitations that significantly affect the evaluation discussed to include software developmental testing or those developmental tests, which will incorporate the system's embedded software?
(a) Configuration Management.
- Have the differences between software functional capabilities of the system to be tested and those of the objective system been identified?
(b) DT&E Objectives.
- Have software test objectives for this phase of testing been stated?
- Has the method for software evaluation been discussed?
(c) DT&E Events, Scope of Testing, and Basic Scenarios.
- Have the key planned software development events been identified?
- Is there a discussion of the analysis, simulations, subsystem tests, and testbeds, which are to be used in determining if software DT&E objectives are met?
- Is there a discussion on software test limitations that may significantly affect the evaluator's ability to draw conclusions and make recommendations concerning software technical parameters?

Part IV. Operational Test and Evaluation (OT&E) Outline

a. OT&E Overview.
(1) Relationship between program schedule, system requirements, and operational issues, reflected?
(2) DT to be used as part of the evaluation identified?
(3) Simulations/models that will be used to supplement OT reflected?
(4) Has logistics support and human performance been addressed?

b. Critical Operational Issues and Criteria.
(1) Approved critical operational issues listed?
(2) Reference made to approved COIC in Annex A?
(3) Have the measures of effectiveness and performance been stated?
(4) Have the evaluation criteria and data requirements for each measure been identified?
(5) Have OT entrance criteria been identified?

c. Future Operational Test and Evaluation.
Evaluations/assessments listed as well as tests?
(1) Configuration Description
(a) Are differences described between tested system and the system to be fielded? For software?
(b) Is the extent of integration/interoperability with other systems reflected?
(c) Has the software and hardware configuration for each test been identified?
(d) Has the degree to which test results from this configuration represent performance of the deployed system been identified?
(2) OT Objectives
(a) Are test objectives including the critical operational issues to be addressed by each phase of OT and the MS(s) stated?
(b) If a Beyond LRIP decision is being supported are test objectives that examine all areas of operational effectiveness and suitability reflected?
(c) Has the relationship between OT objectives and software characteristics which affect critical operational issues been addressed?
(3) OT Events, Scope of Testing, and Scenarios
(a) Scenarios summarized?
(b) Events to be conducted identified?
(c) Type of resources to be used reflected?
(d) Simulation(s)/models to be employed identified?

Figure B–1. Test and evaluation master plan checklist—Continued

(e) Type of representative personnel who will operate and maintain the system reflected?
(f) Status of the logistic support reflected?
(g) Operational and maintenance documentation that will be used identified?
(h) Environment under which the system is to be employed and supported during testing reflected?
(i) Planned sources of information reflected?
(j) Has the relationship between software functions being tested and test scenarios been discussed?
(k) Have load levels to be used, through simulation or other means, and their relationship to the required operational environment been identified?
(l) Has system performance in an operational, electromagnetic environment (EME) been addressed?

(4) Limitations
(a) Are test limitations discussed that may impact the resolution of affected critical operational issues?
(b) Are critical operational issues affected indicated in parentheses after each limitation?
(c) Have any factors which may inhibit realistic OT of the hardware/software been identified?
(d) Have constraints been identified along with their impact on critical operational issues, which impose on software maturity or availability of resources and simulators?
(e) Have waivers been submitted that identify E3/SM operational test limitations?

d. Live Fire Test and Evaluation.
(1) Overall LFT&E strategy reflected?
(2) LFT&E issues identified?
(3) Required levels of system vulnerability/lethality reflected?
(4) Management of LFT&E program identified?
(5) LFT&E schedule reflected?
(6) Funding identified?
(7) Test plans identified?
(8) Requirements reflected?
(9) Related prior and future LFT&E efforts identified?
(10) LFT&E plan identified?
(11) Shot selection process reflected?
(12) Major test limitations identified?

Part V. Test and Evaluation Resource Summary

a. Is a summary of all key T&E resources (government and contractor) provided?

b. Are Major Range and Test Facility Base resources identified?

c. Test Articles.
(1) Are actual number and timing requirements listed?
(2) Are key subsystems to be tested separately and their quantities identified?
(3) Are prototype, development pre-production, or production model use identified?

d. Test Site and Instrumentation.
(1) Are specific test range/facility needs identified?
(2) Are planned test range/facility needs identified as compared with existing and programmed capabilities?
(3) Are new instrumentation acquisitions specified?

e. Test Support Equipment.
(1) Is specifically acquired equipment identified?

Figure B–1. Test and evaluation master plan checklist—Continued

(2) Are unique/special calibration requirements indicated?

f. Threat Representation.
(1) Type/number/availability identified?
(2) Are requirements identified as compared with available and projected assets and their capabilities?
(3) Major shortfalls identified?
(4) Are M&S used as threat systems accredited?

g. Test Targets and Expendables.
(1) Type/number/availability identified for each phase of testing?
(2) Major shortfalls identified?
(3) Threat targets for LFTE identified?
(4) Threat munitions/systems for LFT identified?

h. Operational Force Test Support. Type and timing of aircraft flight hours, and so forth, identified for each phase?

i. Simulations, Models and Testbeds.
(1) System simulations required identified for each phase?
(2) Rationale for usage/application explained?
(3) Accreditation Plan prepared?

j. Special Requirements.
(1) Significant non-instrumentation capabilities and resources discussed?
(2) E3/SM test specific resources addressed?

k. Test and Evaluation (T&E) Funding Requirements.
(1) FY and appropriation line number reflected?
(2) Funding required to pay direct costs identified?
(3) Funding currently appearing in those lines indicated?
(4) Major shortfalls identified?

l. Manpower/Personnel Training. Limitations that affect test execution identified?

Annex A - Bibliography
- Reports documenting developmental and operational T&E reflected?

Annex B - Acronyms

Annex C - Points of Contact

Attachment 1 - Requirements/Test Crosswalk Matrix
- Are COI, MOE, MOS, KPP, CTP, and each DT and OT event represented in the matrix?

Attachment 2 - Critical Operational Isssues and Criteria
- Are the full set of Issue, Scope, Criteria, and Rationale listed?

Figure B–1. Test and evaluation master plan checklist—Continued

Appendix C

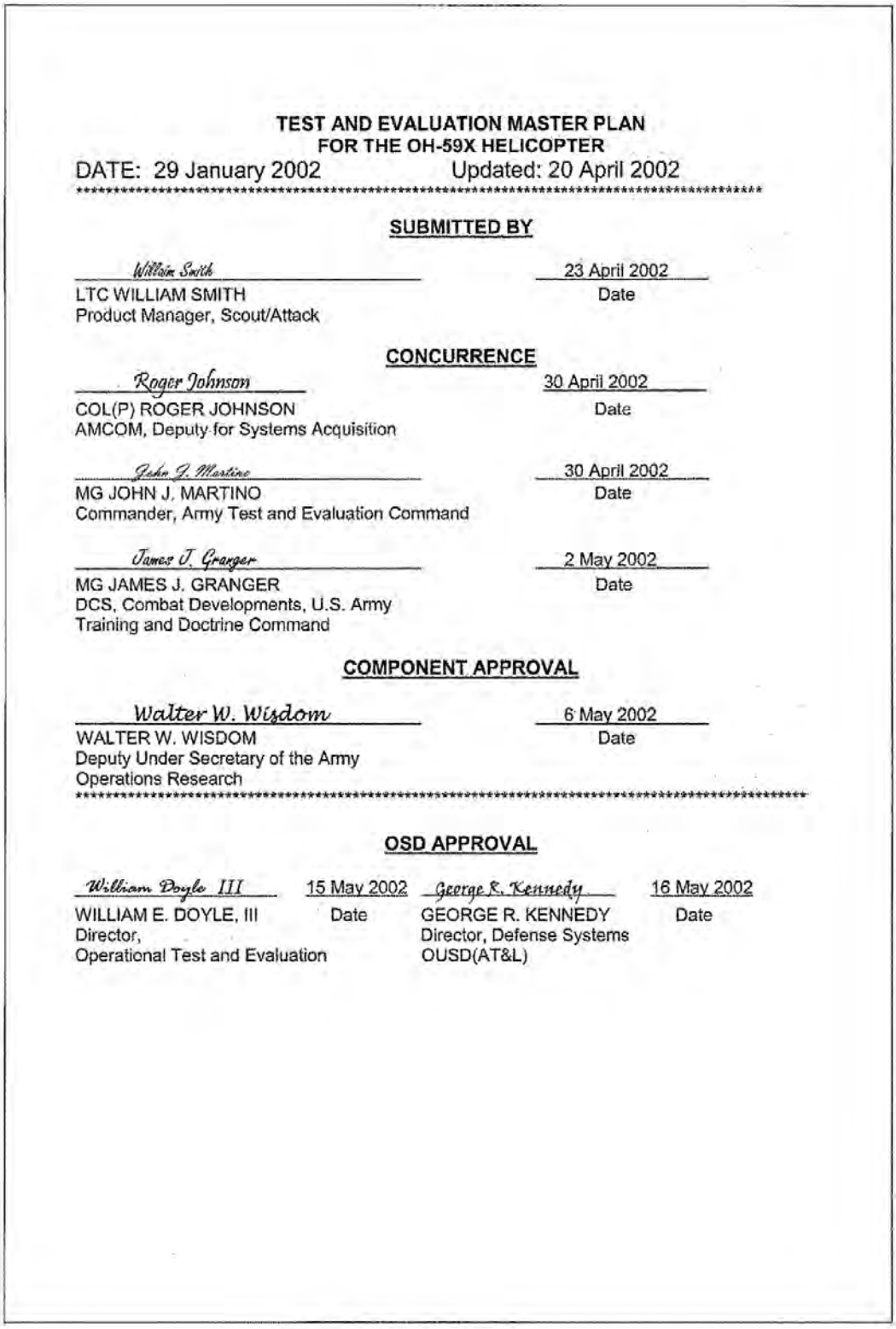
Test and Evaluation Master Plan Approval Pages

C–1. Test and evaluation master plan requirement

Every Army program will have an approved TEMP. TEMP review and approval processes are contained in paragraph 3–5.

C–2. Approval pages

Figures C–1 through C–6 provide the TEMP approval page formats for specific type programs (that is, OSD T&E oversight, non-OSD T&E oversight, and so forth).



TEST AND EVALUATION MASTER PLAN
FOR THE OH-59X HELICOPTER

DATE: 29 January 2002 Updated: 20 April 2002

SUBMITTED BY

William Smith — 23 April 2002
LTC WILLIAM SMITH — Date
Product Manager, Scout/Attack

CONCURRENCE

Roger Johnson — 30 April 2002
COL(P) ROGER JOHNSON — Date
AMCOM, Deputy for Systems Acquisition

John J. Martino — 30 April 2002
MG JOHN J. MARTINO — Date
Commander, Army Test and Evaluation Command

James J. Granger — 2 May 2002
MG JAMES J. GRANGER — Date
DCS, Combat Developments, U.S. Army
Training and Doctrine Command

COMPONENT APPROVAL

Walter W. Wisdom — 6 May 2002
WALTER W. WISDOM — Date
Deputy Under Secretary of the Army
Operations Research

OSD APPROVAL

William Doyle III — 15 May 2002
WILLIAM E. DOYLE, III — Date
Director,
Operational Test and Evaluation

George R. Kennedy — 16 May 2002
GEORGE R. KENNEDY — Date
Director, Defense Systems
OUSD(AT&L)

Figure C–1. Test and evaluation master plan approval page for Office of the Secretary of Defense test and evaluation oversight programs

TEST AND EVALUATION MASTER PLAN
FOR THE
X-42 MISSILE DEFENSE PROGRAM
Update:
20 April 2002

Program Elements

SUBMITTED BY

William Smith — 23 April 2002
COL WILLIAM SMITH, Air Defense — Date
Project Manager, X42 Missile Defense System

CONCURRENCE

Sander D. Patrick — 30 April 2002
DR. SANDER D. PATRICK — Date
PEO, Ballistic Missile Defense Systems
Missile Defense Agency (MDA)

Robert Ironbreaker — 30 April 2002
MG ROBERT IRONBREAKER — Date
Commander, US Army Test and Evaluation Command (ATEC)

James J. Crasher — 2 May 2002
MG JAMES J. CRASHER — Date
Deputy Chief of Staff (DCS) for Development,
U.S. Army Training and Doctrine Command (TRADOC)

Walter W. Wisdom — 16 May 2002
WALTER W. WISDOM — Date
Deputy Under Secretary of the Army
Operations Research

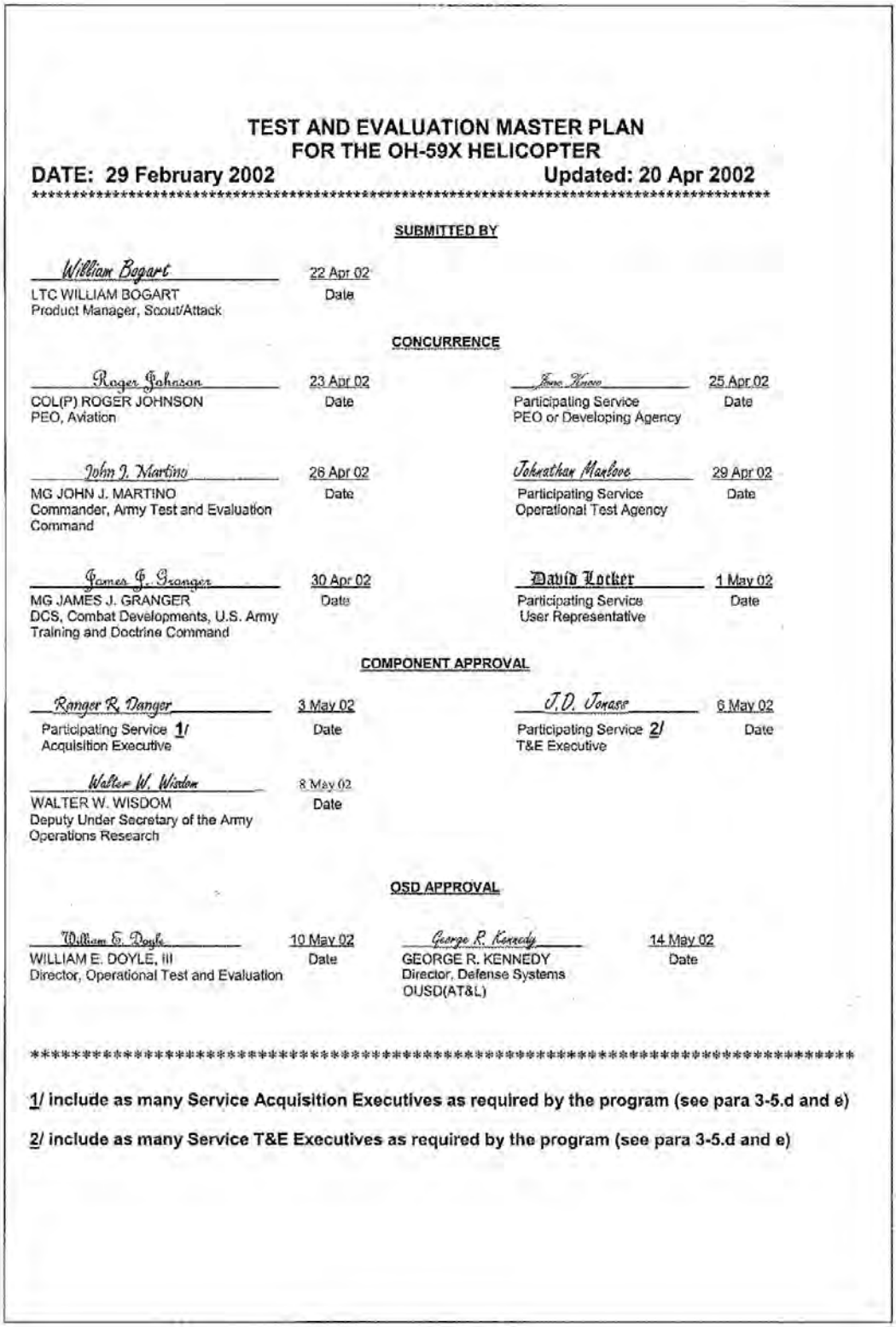
APPROVAL

Franklin R. Pershing — 8 May 2002
LTG FRANKLIN R PERSHING — Date
Director, Missile Defense Agency

Martin Glenn — 8 May 2002
Dr. Martin Glenn — Date
Director, Defense Systems
OUSD(AT&L)

William E. Sotheby — 15 May 2002
WILLIAM E. SOTHEBY — Date
Director, Operational Test & Evaluation

Figure C–2. Test and evaluation master plan approval page for Missile Defense Agency programs



TEST AND EVALUATION MASTER PLAN
FOR THE OH-59X HELICOPTER

DATE: 29 February 2002 Updated: 20 Apr 2002

****

SUBMITTED BY

William Bogart — 22 Apr 02
LTC WILLIAM BOGART, Product Manager, Scout/Attack — Date

CONCURRENCE

Roger Johnson — 23 Apr 02
COL(P) ROGER JOHNSON, PEO, Aviation — Date

[illegible] — 25 Apr 02
Participating Service PEO or Developing Agency — Date

John J. Martino — 26 Apr 02
MG JOHN J. MARTINO, Commander, Army Test and Evaluation Command — Date

Johnathan Marlowe — 29 Apr 02
Participating Service Operational Test Agency — Date

James J. Granger — 30 Apr 02
MG JAMES J. GRANGER, DCS, Combat Developments, U.S. Army Training and Doctrine Command — Date

David Locker — 1 May 02
Participating Service User Representative — Date

COMPONENT APPROVAL

Ranger R. Danger — 3 May 02
Participating Service 1/ Acquisition Executive — Date

J.D. Jonase — 6 May 02
Participating Service 2/ T&E Executive — Date

Walter W. Wisdom — 8 May 02
WALTER W. WISDOM, Deputy Under Secretary of the Army Operations Research — Date

OSD APPROVAL

William E. Doyle — 10 May 02
WILLIAM E. DOYLE, III, Director, Operational Test and Evaluation — Date

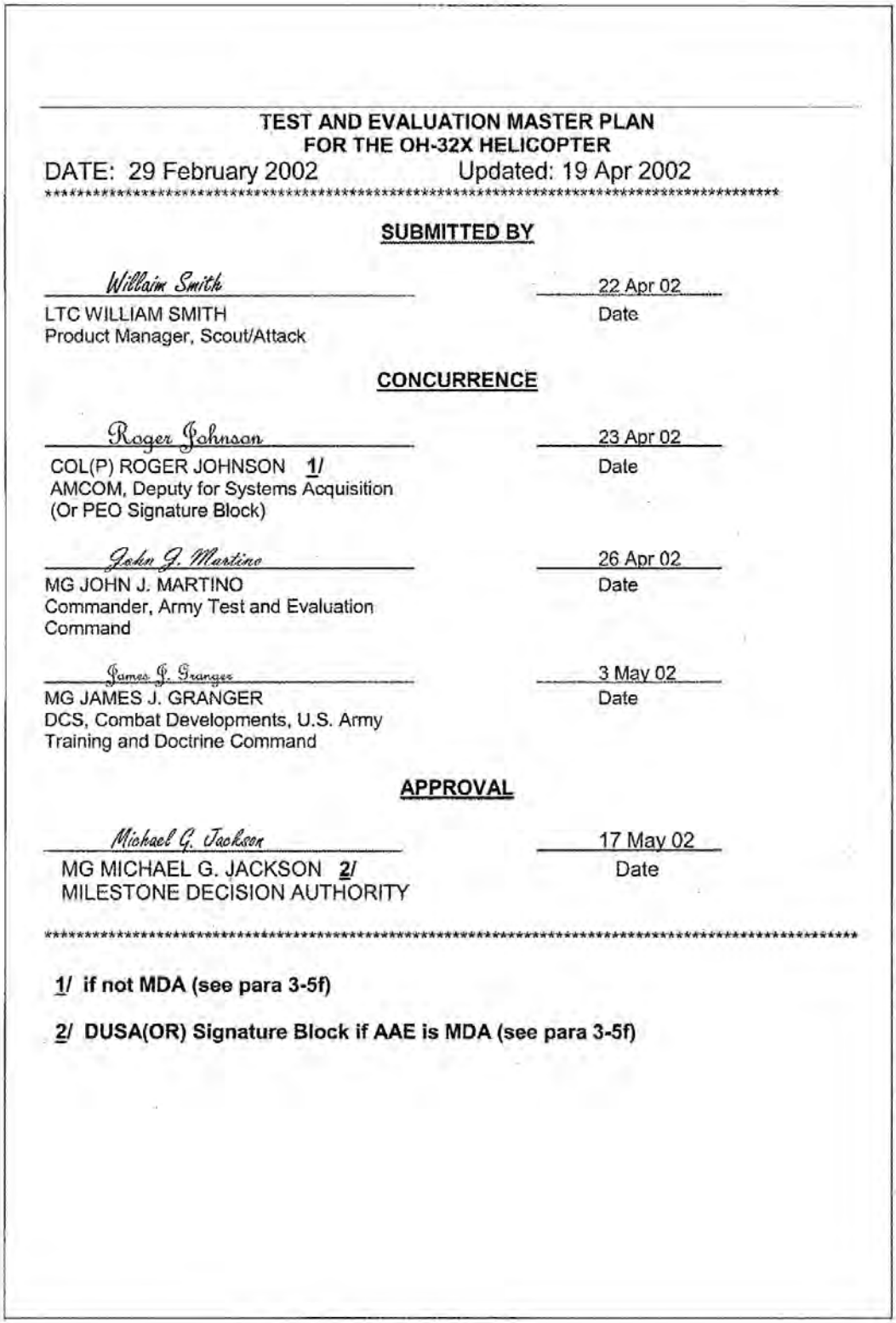
George R. Kennedy — 14 May 02
GEORGE R. KENNEDY, Director, Defense Systems OUSD(AT&L) — Date

****

1/ include as many Service Acquisition Executives as required by the program (see para 3-5.d and e)

2/ include as many Service T&E Executives as required by the program (see para 3-5.d and e)

Figure C–3. Test and evaluation master plan approval page for multi-Service Office of the Secretary of Defense test and evaluation oversight programs



TEST AND EVALUATION MASTER PLAN
FOR THE OH-32X HELICOPTER

DATE: 29 February 2002 Updated: 19 Apr 2002

SUBMITTED BY

William Smith — 22 Apr 02
LTC WILLIAM SMITH — Date
Product Manager, Scout/Attack

CONCURRENCE

Roger Johnson — 23 Apr 02
COL(P) ROGER JOHNSON 1/ — Date
AMCOM, Deputy for Systems Acquisition
(Or PEO Signature Block)

John J. Martino — 26 Apr 02
MG JOHN J. MARTINO — Date
Commander, Army Test and Evaluation
Command

James J. Granger — 3 May 02
MG JAMES J. GRANGER — Date
DCS, Combat Developments, U.S. Army
Training and Doctrine Command

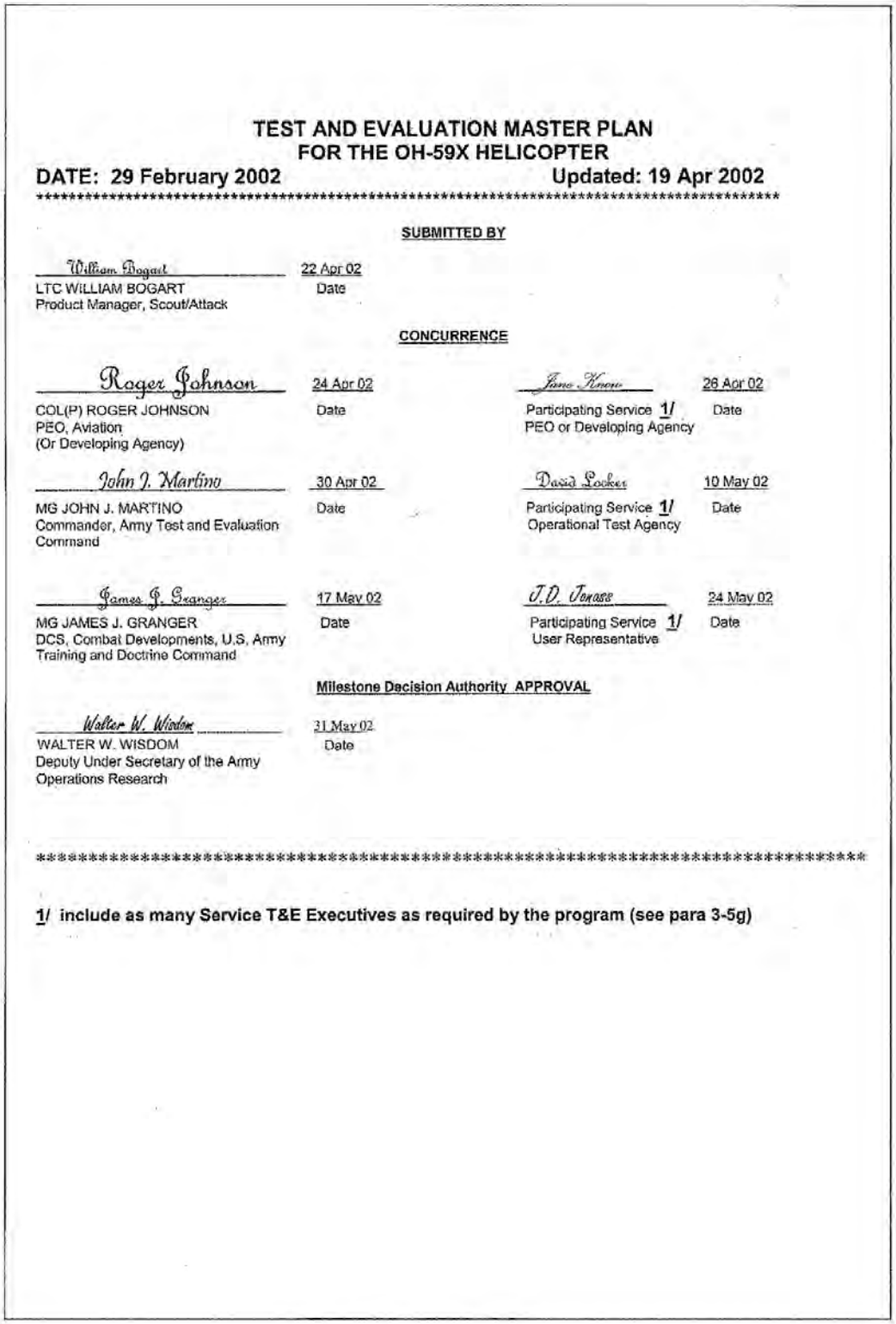
APPROVAL

Michael G. Jackson — 17 May 02
MG MICHAEL G. JACKSON 2/ — Date
MILESTONE DECISION AUTHORITY

1/ if not MDA (see para 3-5f)

2/ DUSA(OR) Signature Block if AAE is MDA (see para 3-5f)

Figure C–4. Test and evaluation master plan approval page for Acquisition Category II non-Office of the Secretary of Defense test and evaluation oversight programs



TEST AND EVALUATION MASTER PLAN
FOR THE OH-59X HELICOPTER

DATE: 29 February 2002 **Updated: 19 Apr 2002**

****

SUBMITTED BY

William Bogart — 22 Apr 02
LTC WILLIAM BOGART — Date
Product Manager, Scout/Attack

CONCURRENCE

Roger Johnson — 24 Apr 02
COL(P) ROGER JOHNSON — Date
PEO, Aviation
(Or Developing Agency)

Jane Knorr — 26 Apr 02
Participating Service 1/ — Date
PEO or Developing Agency

John J. Martino — 30 Apr 02
MG JOHN J. MARTINO — Date
Commander, Army Test and Evaluation Command

David Lockey — 10 May 02
Participating Service 1/ — Date
Operational Test Agency

James J. Granger — 17 May 02
MG JAMES J. GRANGER — Date
DCS, Combat Developments, U.S. Army Training and Doctrine Command

J.D. Jones — 24 May 02
Participating Service 1/ — Date
User Representative

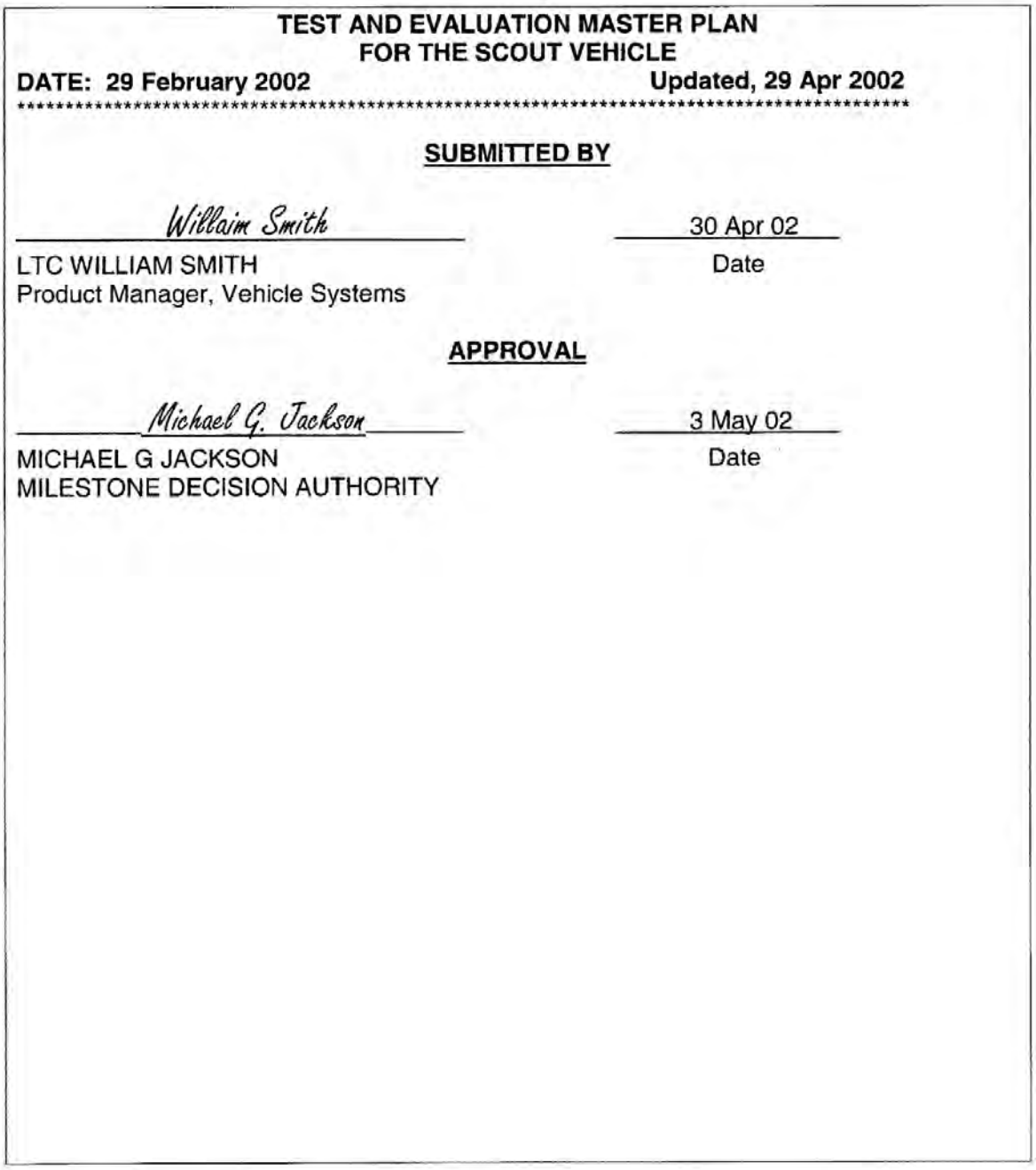
Milestone Decision Authority APPROVAL

Walter W. Wisdom — 31 May 02
WALTER W. WISDOM — Date
Deputy Under Secretary of the Army
Operations Research

****

1/ include as many Service T&E Executives as required by the program (see para 3-5g)

Figure C–5. Test and evaluation master plan approval page for multi-Service non-Office of the Secretary of Defense test and evaluation oversight Acquisition Category II programs, Army lead, and milestone decision authority is Army Acquisition Executive



TEST AND EVALUATION MASTER PLAN
FOR THE SCOUT VEHICLE

DATE: 29 February 2002 Updated, 29 Apr 2002

****

SUBMITTED BY

William Smith — 30 Apr 02

LTC WILLIAM SMITH — Date
Product Manager, Vehicle Systems

APPROVAL

Michael G. Jackson — 3 May 02

MICHAEL G JACKSON — Date
MILESTONE DECISION AUTHORITY

Figure C–6. Test and evaluation master plan approval page for Acquisition Category III non-Office of the Secretary of Defense test and evaluation oversight programs

Appendix D

Test and Evaluation Master Plan Format and Content

D–1. Part I—System Introduction

a. Mission description. Reference the MNS, CRD (if applicable), C4ISP, and ORD. Briefly summarize the mission need described therein. Specifically—

(1) Define the need in terms of mission, objectives, and general capabilities.

(2) Summarize from paragraph 2, MNS.

(3) Describe the natural environment in two aspects; logistically and operationally. Summarize from paragraph 4, MNS.

(4) For non-tactical C4/IT programs, system capabilities are detailed in paragraphs 2 and 4 of the MNS and part 1, section 4 of the System Decision Paper. Functional process improvement is detailed in chapter 3 of the MNS or part 2, section 1 of the System Decision Paper.

(5) Include a description of the operational and logistical environment envisioned for the system.

b. System description. Provide a brief description of the system design, to include the following items:

(1) Key features and subsystems, both hardware and software (such as integrated architecture, interfaces, security levels, and reserves), which allow the system to perform its required operational mission.

(2) Interfaces with existing or planned systems that are required for mission accomplishment. Address relative maturity, integration, and modification requirements for non-developmental items. Include interoperability with existing and/or planned systems of other DoD Components or allies. Provide a diagram of the operational, technical, and systems views of the integrated architecture.

(3) Critical system characteristics or unique training and logistical support concepts resulting in special test and analysis requirements (for example, PDSS; hardness against nuclear effects; resistance to countermeasures; resistance to reverse engineering/exploitation efforts (anti-tamper); development of new threat simulations, simulators, or targets).

(a) For MS B summarize from the ORD or development specification, if available.

(b) For MS C and beyond summarize from the development specification.

(c) Include a description of what constitutes the IOC and the final operational capability for the system.

(4) Non-tactical C4/IT programs.

(a) Key features of the total system are identified in the Defense Information Infrastructure common operating environment, or section 3 of the System Specification (DI–CMAN–80008A), as applicable.

(b) Interfaces are identified in chapter 4–C of the MNS, or section 3.2 of the optional user's functional description (UFD), and section 3 of the System Specification, or in section 3 of the Interface Requirements Specification (DI–MCCR–80026A), as appropriate.

(c) Unique system characteristics are identified in chapter 4–A of the MNS.

c. System threat assessment. Reference the STA and summarize the threat environment described therein as follows:

(1) Summarize the operational threat environment from paragraph 4a, STAR, and the system specific threat from paragraph 4e, STAR.

(2) Include the threat at IOC, follow-on—at IOC plus 10 years, and the reactive threat from paragraph 4e and 4f, STAR, if applicable. If the other sections of the TEMP are unclassified, then keep this section unclassified.

(3) For non-tactical C4/IT programs, this is not applicable for IT systems unless they are developed to counter a specific threat.

d. Measures of effectiveness and suitability. List the performance (operational effectiveness and suitability) capabilities identified as required in the ORD. The capabilities identified in table D–1 are not intended to represent all capabilities related to the MOE and MOS. MOE and MOS should be identified to ensure that the TEMP adequately establishes the needed basis for T&E of the system's operational effectiveness and suitability. The critical operational effectiveness and suitability parameters and constraints must crosswalk to those used in the AoA, and include manpower, personnel, training, software, computer resources, infrastructure requirements, transportation (lift), compatibility, Army or Joint interoperability and integration, IA, E3, and spectrum supportability. Focus on operational capabilities, not design specifications (such as weight and size). Limit the list to critical metrics that apply to capabilities essential to mission accomplishment. Include and clearly identify all KPP. For each listed parameter, provide the threshold and the objective values from the ORD and the ORD reference. If the system evaluator determines that the required capabilities and characteristics contained in the ORD provide insufficient measures for an adequate

evaluation and OT, the system evaluator proposes additional measures through the IPT process. Upon receipt of such a proposal, the ORD approval authority will establish the level of required performance characteristics. Specifically—

(1) Summarize from the ORD paragraphs 4, 5, and 6.

(2) For ACAT III programs not designated for OSD T&E oversight, it is sufficient to reference the ORD.

(3) Non-tactical C4/IT programs.

(a) In cases when the optional UFD is used, operational requirements are amplified in the UFD, or in sections 3.5.2 and 3.7–3.12 of the Software Requirements Specification (DI–MCCR–80025A).

(b) For systems using accelerated techniques and automated tools, use the ORD and Software Requirements Specification.

Table D–1
Measures of effectiveness and suitability

Operational requirement	Parameter	ORD threshold	ORD objective	ORD reference
Mobility	Land Speed** Miles per hour on secondary roads **KPP	xx miles per hour	xx miles per hour	Paragraph xxx
Firepower	Accuracy Main Gun Probability of hit/ stationary platform/ stationary target	xxx probability of hit @ xxx range	xxx probability of hit @ xxx range	Paragraph xxx
Interoperability	Interoperable with Current and Planned Secure Voice and Data Communications Systems **(KPP)	Meet 100% of the critical top level information exchange requirements	Same as threshold	4(b)
Supportability	Reliability Mean Time Between Opn'tl Mission Failure	xxx hours	xxx hours	Paragraph xxx

e. Critical technical parameters.

(1) List in a matrix format (see table D–2) the CTPs of the system (including software maturity and performance measures) that will be evaluated (or reconfirmed if previously evaluated) during the remaining phases of DT. Include the system interoperability criteria, maturity criteria, and performance exit criteria necessary for operational test readiness certification. CTP are derived from the ORD, critical system characteristics and technical performance measures and should include the parameters in the APB. CTP are measurable critical system characteristics that, when achieved, allow the attainment of operational performance requirements. They are not ORD requirements. Rather, they are technical measures derived from ORD requirements. Failure to achieve a CTP should be considered a reliable indicator that the system is behind in the planned development schedule or will likely not achieve an operational requirement. Limit the list of CTPs to those that support critical operational requirements. The system specification is usually a good reference for the identification of CTPs.

(2) Next to each technical parameter, list a threshold for each stage of development. Developmental test events are opportunities to measure the performance of the system as it matures. For most technical parameters, the listed thresholds should reflect growth as the system progresses toward achieving its ORD requirements. Also, list the decision supported after each event to highlight technical performance required before entering the next acquisition or operational test phase.

(3) Ensure technical parameters are included for technical interoperability.

(4) Software CTPs will comply with the latest version of the JTA-Army including language, architecture, interfaces, supportability, security levels, time, memory, and input/output reserves.

(5) At MS B, the initial TEMP is not expected to contain detailed requirements. The TEMP update in support of MS C should include detailed values.

Table D–2
Critical technical parameters

Supported operational requirement[1]	Technical parameter	Developmental stage event	Threshold value	Decision supported
In most cases a measure of effectiveness or suitability from paragraph 1.d	Technical measures derived to support operational requirement	Developmental stage events (Described in TEMP Part III) designed to measure system performance against technical parameters.	Minimum value required at each developmental event. Most parameters will show growth as the system progresses through testing. Final value should reflect level of performance necessary to satisfy the operational requirement.	May be any decision marking the entrance into a new acquisition phase or may be a readiness for operational test decision.
Example: Main Gun Probability of Hit, 94% at 1,500 meters (ORD para. xxx.x)	Example: Auxiliary sight Boresight accuracy	Example: System demo Test-accuracy test Prod readiness Test-accuracy Prod qual test	Example: +/- 5 mils +/- 3 mils +/- 1 mil	Example: Milestone B MS C (Low Rate Initial Production Decision) FRP DR

Notes:
[1] Include ORD reference.

(6) For tactical C4I/IT non-OSD T&E oversight systems and when intra-Army interoperability is identified as an operational requirement, there should be a measurable critical system intra-Army interoperability characteristic, in order to complete required intra-Army interoperability certification testing. Preferably, this interoperability characteristic should include at least one CTP.

(7) Non-tactical C4/IT programs.

(a) In addition to the references listed above, also reference section 3.6 of the Software Specification (DI–MCCR–80025A), as applicable.

(b) The CTP table for IT programs is similar in format to the CTP table for materiel systems with column headings and descriptions as follows:

1. CTPs are obtained from the software specification and other related documents. For systems using accelerated techniques and automated tools, CTPs are derived from the System/Subsystem Specifications and its versions transitioning to become the optional UFD.
2. Reference the source from which the parameter and value is derived.
3. Total events.
4. Technical Objective for each test event.
5. Location.
6. Schedule—the fiscal quarter when the test will be initiated.
7. Decision Supported.
8. Demonstrated Value.

D–2. Part II—Integrated Test Program Summary

a. Integrated test program schedule.

(1) As illustrated in figure D–1 (can be a fold-out chart), display the integrated time sequencing of the critical T&E phases and events, related activities, and planned cumulative funding expenditures by appropriation.

(a) The integrated test program schedule will be divided into seven major areas: program milestones; program acquisition events; contract release and awards; program deliverables; developmental tests; live fire tests; operational tests; and program funding.

(b) The schedule must cover the acquisition and T&E program through full operational capability.

(2) Include event dates such as MS decision points; operational assessments, test article availability; software version releases; appropriate LFT&E, and operational and developmental test events; SERs, long lead items dates, LRIP

deliveries; FRP deliveries; IOC; final operational capability; and statutorily required reports such as the LFT&E report and BLRIP report.

(3) A single schedule should be provided for multi-Service or Joint and Capstone TEMPs showing all DoD Component system event dates.

(4) For ACAT III programs not on the OSD T&E Oversight List, it is not critical to adhere to the exact format of figure D–1. A chart showing the program MSs and the planned tests is adequate.

(5) For tactical C4I/IT non-OSD T&E oversight systems, identify the DT and OT events, if applicable, that will be used to support the CTSF testing and the CIO/G–6 (or delegated MDA) intra-Army interoperability certification in support of acquisition DRs, OT, and materiel release entrance criteria. DT and OT results can also be leveraged by the JITC to facilitate the issuance of a joint interoperability certification.

(6) For non-tactical C4/IT programs, information/data should be obtained from the master schedule, section F, of the Management Plan (MP).

(7) Funding expenditures. Provide annual amounts allocated or requested/estimated (outside POM funding years) for RDT&E and production accounts. Further identify projected expenditures, obtained from MRTFB Commanders, for the use of MRTFB ranges and facilities that come from within the program RDT&E budget line.

b. Management.

(1) Discuss the T&E responsibilities of all participating organizations (that is, developers, testers, evaluators, and users), to include the following:

(a) Identify T&E WIPT members and their role (see table D–3). Reference the T&E WIPT Charter for specific responsibilities. (See AR 73–1 and chap 2 of this pamphlet.) The T&E WIPT Charter must be included as a reference in annex A, the bibliography of the TEMP.

(b) For ACAT III programs not designated for OSD T&E oversight, it is sufficient to reference the T&E WIPT Charter.

(2) Provide the date (fiscal quarter) when the decision to proceed beyond-LRIP is planned. LRIP quantities required for operational test must be identified for DOT&E approval prior to MS C for ACAT I programs and other ACAT programs designated for DOT&E OT oversight. The date for the BLRIP decision is found in the integrated program summary, acquisition strategy report.

(a) The quantity of LRIP items needed for IOT is recommended by ATEC in coordination with the PM.

(b) The quantity of items needed for IOT for all other ACAT programs are included as recommended by ATEC.

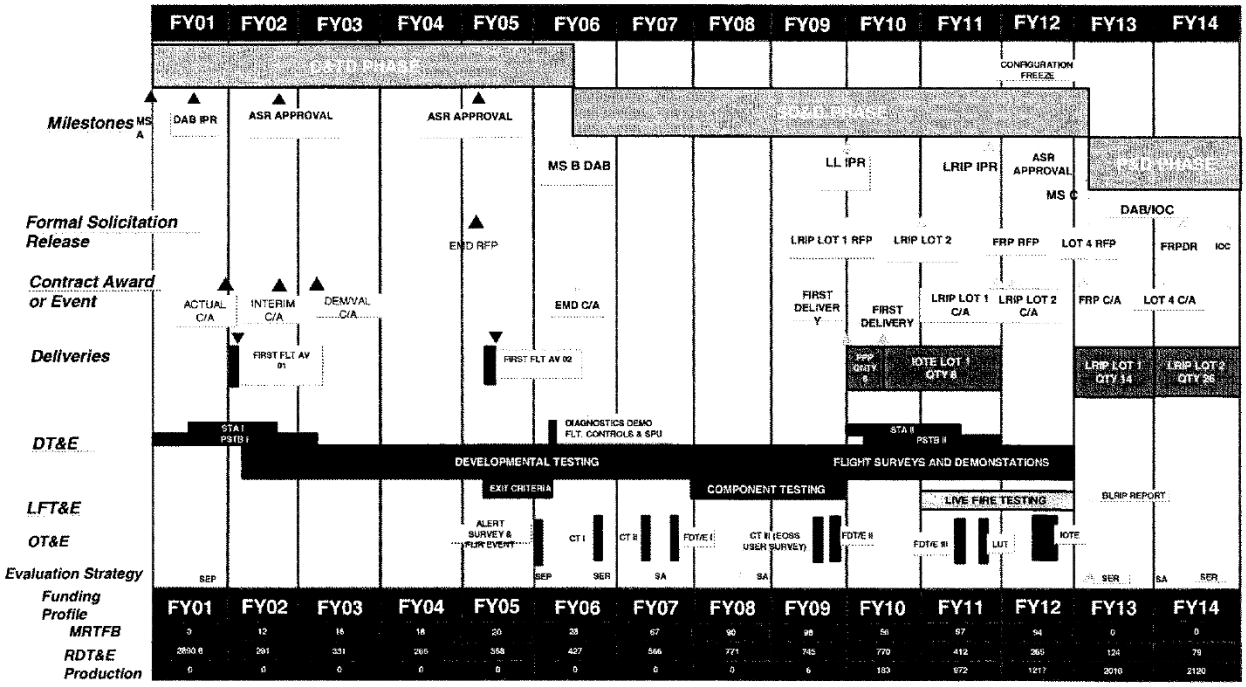


Figure D–1. Integrated test program summary

Table D–3
Test and evaluation working-level integrated product team membership and roles

T&E WIPT member	T&E WIPT role
Program manager (any given system)	T&E WIPT chair
TRADOC proponent school	System combat developer
AEC	Independent system evaluator
DTC or other DT activity	System developmental tester
OTC or other OT activity	System operational tester
ASA (ALT) ILS	Independent logistician
SLAD ARL	Survivability/lethality analyst
Joint Spectrum Center	E3 and spectrum management
TI	Threat integrator
TRADOC training proponent	System trainer
ASA (ALT)	HQDA representative
CIO/G–6	Same as above
DUSA (OR)	Same as above
ASA (ALT) ILS	Same as above
DCS, G–8	Same as above
DCS, G–4	Same as above
DCS, G–2	Same as above
DCS, G–1	Same as above
Air Force Operational Test and Evaluation Center	Participating Service operational test representative if T&E WIPT has multi-Service participation.
Marine Corps Operational Test and Evaluation Agency	Same as above
Operational Test and Evaluation Force (Navy)	Same as above
Participating service user representative	Additional combat developer input
Associate members (as appropriate)	

(1) Identify and discuss any operational issues and vulnerability and lethality live fire test requirements that will not be addressed before proceeding beyond LRIP.

(2) Identify the technological maturity of the technology being designed into the system and components/parts/subsystems. State the proven methods of test and calibration associated with test to ensure that the system and components/parts/subsystems are testable in operation and support environments. State any deficiencies and how the deficiencies will be resolved prior to OT and production.

(3) For tactical C4I/IT non-OSD T&E oversight systems, identify the specific intra-Army interoperability responsibility of the PM/system manager; DCS, G–3; TSM; CTSF; CECOM's Software Engineering Center; Digital Integration Laboratories; and other organizations, as applicable. In addition, list the intra-Army interoperability exit criteria for the upcoming acquisition DRs.

(4) Provide the proposed or approved performance exit criteria to be assessed at the next acquisition decision. For a TEMP update, generated by an APB breach or significant change, provide the acquisition decision memorandum-approved exit criteria from the current phase's beginning milestone decision, or any revised ones generated by the breach or the significant change.

(5) For non-tactical C4/IT programs, provide the date (fiscal quarter) when the decision to proceed to FRP DR interoperability certification is planned. If the system is being developed through an incremental acquisition strategy, provide the date (fiscal quarter) when the decision to proceed to FRP DR interoperability certification is planned and briefly outline the extent of incremental deployment activities prototype, test bed sites, and so forth prior to FRP DR

interoperability certification. The extent of incremental deployment before IOT&E must be identified prior to MS C for OSD and Army MAIS systems.

D–3. Part III—Developmental Test and Evaluation Outline

a. Developmental test and evaluation overview. Explain how DT&E will verify the status of engineering and manufacturing development progress; verify that design risks have been minimized; antitamper provisions have been implemented (required security designs and security controls were implemented); substantiate achievement of contract technical performance requirements; and certify readiness for dedicated operational test. Specifically—

(1) Identify any technology/subsystem that has not demonstrated its ability to contribute to system performance and ultimately fulfill mission requirements.

(2) Identify the degree to which system hardware and software design has stabilized so as to reduce manufacturing and production decision uncertainties.

(3) Assess the degree to which system software has stabilized so as to reduce software rework required.

(4) Identify how system hardware-in-the-loop, simulations, training simulators, flight mission simulators, and the system test support base will be used to support OT, wartime problem resolution, and system upgrades through the life cycle of the system.

(5) For tactical C4I/IT non-OSD T&E oversight systems, address how the intra-Army interoperability CTPs is being verified for technical performance requirements and how it can be used to certify interoperability readiness for dedicated OT.

(6) For non-tactical C4/IT programs, show how the metrics in each phase relate to those in previous and subsequent phases.

b. Future developmental test and evaluation. Discuss all remaining DT&E that is planned, beginning with the date of the current TEMP revision and extending through completion of production. Whenever possible, DT results should be made available to the JITC in an attempt to minimize the cost of joint interoperability testing. Place emphasis on the next phase of testing. For each phase, include—

(1) Configuration description. Summarize the functional capabilities of the system's developmental configuration and how they differ from the production model.

(2) DT&E objectives. State the test objectives for this phase in terms of the CTPs to be confirmed, to include antitamper characteristics. Identify any specific technical parameters that the MDA has designated as exit criteria and/or directed to be demonstrated in a given phase of testing.

(3) DT&E events, scope of testing, and basic scenarios. Summarize the test events, test scenarios and the test design concept. Quantify the testing (for example, number of test hours, test events, and test firings). List the specific threat systems, surrogates, countermeasures, component or subsystem testing, and testbeds that are critical to determine whether or not developmental test objectives are achieved. As appropriate, particularly if an agency separate from the test agency will be doing a significant part of the evaluation, describe the methods of evaluation. List all models and simulations to be used to evaluate the system's performance, explain the rationale for their credible use and provide their source of VV&A. Describe how performance in natural environmental conditions representative of the intended area of operations (for example, temperature, pressure, humidity, fog, precipitation, clouds, electromagnetic environment, blowing dust and sand, icing, wind conditions, steep terrain, wet soil conditions, high sea state, and storm surge and tides) and interoperability with other weapon and support systems, as applicable, to include insensitive munitions, will be tested. Describe the DT&E plans and procedures that will support the JITC/DISA joint interoperability certification recommendation to the Director, Joint Staff (J–6) in time to support the FRP DR. Joint and combined interoperability certification will be directly coordinated through the APTU at the CECOM Software Engineering Center. For Army-approved systems, discuss the DT&E plans and procedures that will support the CTSF interoperability certification recommendation to the CIO/G–6 or TEMP approval authority. Topics addressed in this section can include—

(a) Early developmental tests that will be performed to mitigate technical risks in the program that are defined in the Risk Assessment, annex D, Integrated Program Summary.

(b) Identification of developmental tests that will be used to demonstrate that the test item is safe and that the TMs are verified and validated and ready for use in a follow-on or concurrent operational test.

(c) Identification of the test, usually the PQT, that will be performed to validate that the system meets the system's technical performance requirements that are usually contractually mandated in a specification.

(d) The developmental tests that will be used to certify the system is ready for IOT and who has responsibility for execution.

(e) If applicable, testing to address conventional weapon effects, E3, electronic countermeasures, electronic counter-countermeasures, initial nuclear weapons effects (NWE), advanced technology survivability, and NBC contamination survivability (see DoDI 5000.02).

(f) Identification of the developmental test plans and strategy to prove or validate the manufacturing process (see DoDI 5000.02).

(4) The following areas (specifically the description and objective) of each of the developmental tests addressed in future DT&E:

(a) RAM.

(b) Electromagnetic compatibility (EMC) and RF management.

(c) Human systems integration/MANPRINT.

(d) Environmental safety and occupational health.

(e) Integrated logistical support. A LD is required for all acquisition programs unless waived. (See AR 700–127.) The waiver, if approved, will be documented in part II, section 2 of the TEMP, with the approval document referenced in annex A, bibliography of the TEMP.

(f) Discuss the indicators that will be used to determine software status and evaluate progress toward software maturity in support of key decision points, particularly for software intensive systems. Show how the indicators in each phase relate to those in previous and subsequent phases.

(g) Include a discussion of any test databases and/or remote terminal emulators to be used and their relationship to the objective system environment.

(5) For non-tactical C4/IT programs, the following software tests must be addressed, with specific test items listed below each test type:

(a) Software development test.

1. Configuration description (of test item).
2. T&E objectives.
3. Events, scope of testing, and basic scenarios.
4. Limitations.

(b) Software qualification test (SQT).

1. Configuration description (of test item).
2. T&E objectives.
3. Events, scope of testing, and basic scenarios.
4. Limitations.

(6) Limitations. Discuss the test limitations that may significantly affect the evaluator's ability to draw conclusions, state the impact of these limitations, and explain resolution approaches.

(7) For tactical C4I/IT non-OSD T&E oversight systems, describe the set of approved CTSF test requirements, criteria for intra-Army interoperability testing, and DT events that will be used to satisfy both intra-Army and joint interoperability certification test requirements. Identify future DT that will address the remaining intra-Army interoperability requirements.

D–4. Part IV—Operational Test and Evaluation Outline

a. Operational test and evaluation overview.

(1) The primary purpose of OT and system evaluation is to determine whether systems are operationally effective, suitable, and survivable for the intended use by representative users in a realistic environment before production or deployment.

(2) The TEMP will show how program schedule, test management structure, and required resources are related to the system evaluation strategy. OT will provide data to support the system evaluation and will be conducted with typical users in an environment as operationally realistic as possible, including threat representative opposing forces and the expected range of natural environmental conditions.

(3) Summarize the entire OT&E program. The purpose of the overview is to give a quick, concise look at the overall system evaluation strategy and the test program and M&S to support it, explaining the many interrelationships and opportunities to conduct CE. Topics that can be addressed include—

(a) Description of the overarching evaluation model being used.

(b) Definitions of mission effectiveness, suitability, and survivability.

(c) Identification of mission tasks that the system is expected to enhance.

(d) Identification of the system function capabilities that the system is expected to possess.

(e) Key technical and operational characteristics of the system that will be the focus of the system evaluation.

(f) Identification of contractor and developmental tests that will be used as part of a system evaluation or assessment.

(g) Identification of models and simulations that will be used to supplement and extend OT as part of a system evaluation or assessment.

(h) Identification of completed and planned Battle Lab Experimentation to be used in the system evaluation. These experiments when planned and executed in coordination with ATEC may serve to reduce future operational test requirements.

(i) Sources of data, baseline comparisons, general analysis scheme, test data, and AoA linkage.

(4) For tactical C4I/IT non-OSD T&E oversight systems, address both the intra-Army and joint interoperability operational effectiveness issues and criteria, if applicable. Moreover, ensure that entrance criteria for operational tests address CTSF communications/data interfaces test results and the criteria for both intra-Army and joint interoperability.

b. Critical operational issues and criteria. List in this paragraph the approved COIC. COIC include operational effectiveness, suitability, and survivability issues that must be examined to evaluate/assess the system's capability to perform its mission.

(1) State the MOEs and MOPs. Define the data requirements for each MOE and MOP.

(2) Include the approved COIC in their entirety in the TEMP or as Attachment 2 including Issue, Scope, Criteria, and Rationale.

(3) Reference the COIC approval document in annex A, bibliography, of the TEMP.

(4) For tactical C4I/IT non-OSD T&E oversight systems, include, if appropriate, at least one intra-Army interoperability operational effectiveness issue and criterion.

c. Future operational test and evaluation. For each remaining phase of operational test, separately address the following:

(1) *Configuration description.* Identify the system to be tested during each phase, and describe any differences between the tested system and the system that will be fielded. Include, where applicable, software maturity performance and criticality to mission performance, and the extent of integration with other systems with which it must be interoperable or compatible. Characterize the system (for example, prototype, engineering development model, production representative or production configuration).

(2) *Operational test and evaluation objectives.* State the test objectives, including the objectives and thresholds and critical operational issues, to be addressed by each phase of OT&E and the decision points supported. OT&E that supports the FRP DR will have test objectives, to include anti-tamper characteristics that interface with operations and maintainers, and that resolve all unresolved effectiveness, suitability, and survivability COI.

(3) *Operational test and evaluation events, scope of testing, and scenarios.* Summarize the scenarios and identify the events to be conducted, type of resources to be used, the threat simulators and the simulations to be employed, the type of representative personnel who will operate and maintain the system, the status of the logistic support, the operational and maintenance documentation that will be used, the environment under which the system is to be employed and supported during testing, the plans for interoperability and compatibility testing with other United States/Allied systems, the anti-tamper characteristics to be assessed in an operational environment and support systems as applicable. Identify planned sources of information (for example, DT, testing of related systems, and M&S) that may be used by the operational tester to supplement this phase. Whenever models and simulations are to be used: Identify the planned M&S; explain how they are proposed to be used; and provide the source and methodology of the VV&A underlying their credible application for the intended use. If OT cannot be conducted or completed in this phase of testing and the outcome will be an assessment instead of an evaluation, this will clearly be stated and the reasons explained. Describe the OT&E plans and procedures that will support JITC/DISA (OSD T&E oversight and Joint systems) joint interoperability certification recommendation to the Director, Joint Staff (J–6) in time to support the FRP DR. Joint and combined interoperability certification will be specifically coordinated through the APTU at the CECOM Software Engineering Center. For Army approved systems, discuss the U.S. Army CTSF interoperability certification recommendation submitted to the CIO/G–6.

(4) *Areas to address.* The following areas need to be addressed (specifically, the description and objective) of each of the operational tests addressed in this section.

(a) Human performance issues.

(b) Logistics support issues (readiness and RAM) to include TMDE, automatic test equipment, test program sets, test and calibration interface devices, calibration equipment, calibration spheres and methods, and integrated diagnostics.

(c) Identify operational tests that will be conducted and the developmental tests that will provide source data for the system evaluation or assessment. When developmental tests are identified, subparagraph (6) Operational Test and

Evaluation Events, Scope of Testing, and Scenarios, should define the data in general terms that will be taken from the developmental test for the system evaluation or assessment. This will ensure that the developmental testers, by their signature on the TEMP, have agreed to collect and provide that data to the system evaluator.

(d) Describe how models will be accredited for use in specific operational tests. The approval vehicle for accreditation is an Accreditation Plan as outlined in AR 5–11. Reference the accreditation plan in annex A, bibliography of the TEMP. Part V of the TEMP, Test and Evaluation Resource Summary, will identify the resources necessary to perform the validation and/or accreditation.

(5) *Limitations.* Discuss the T&E limitations including threat realism, resource availability, limited operational (military, climatic, and nuclear) environments, limited support environment, maturity of tested system, and safety that may impact the resolution of affected critical operational issues. Indicate the impact of the limitations on the ability to resolve critical operational issues and the ability to formulate conclusions regarding operational effectiveness, suitability, and survivability. Indicate the critical operational issues affected in parenthesis after each limitation.

(6) *For tactical C4I/IT non-Office of the Secretary of Defense test and evaluation oversight systems.* Identify remaining phases of OT and both intra-Army and joint interoperability operational effectiveness issues and criteria that will be addressed. Describe the configuration of the future systems and the remaining intra-Army interoperability operational effectiveness issues and criteria.

d. Live fire test and evaluation. This paragraph applies to those systems that are identified as a covered system or major munitions program as defined in 10 USC 4172. Do not address LFT&E in a separate annex.

(1) See also the Defense Acquisition Guidebook. Include a description of the overall LFT&E strategy for the system; critical LFT&E issues; required levels of system protection and tolerance to terminal effects of threat weapons and lethality; the management of the LFT&E program; LFT&E schedule, funding plans and requirements; related prior and future LFT&E efforts; the evaluation approach and shot-lines selection process; M&S strategy and VV&A; and major T&E limitations for the conduct of LFT&E. Discuss, if appropriate, procedures intended for obtaining a waiver from full-up, system-level live fire testing (realistic survivability/lethality testing as defined in 10 USC 4172) before entry into the System Development and Demonstration Phase. LFT&E resource requirements (including test articles and instrumentation) will be appropriately identified in part V (Test and Evaluation Resource Summary) of the TEMP.

(2) Group all vulnerability/lethality testing (when applicable) under one paragraph to show how the vulnerability/lethality issue is being assessed through various tests and subtests. Such testing can include dedicated tests such as ballistic hull and turret testing. Subtests can include armor plate tests, penetration tests, as well as other tests that validate the vulnerability/lethality requirements of a program.

(3) Future LFT&E is discussed at the same level of detail as DT&E and OT&E. Discuss each live fire test phase, the configuration description, test objectives, scope of testing, and limitations.

(4) Include an LFT&E planning matrix that covers all tests within the LFT&E strategy, their schedules, the issues they will address and which planning documents proposed for submission to DOT&E for approval and which are proposed to be submitted for information and reviews only.

D–5. Part V—Test and Evaluation Resource Summary

Provide a summary (preferably in table or matrix format) of all key T&E resources, both Government and contractor, that will be used during the course of the acquisition program. The initial TEMP at program initiation should project the key resources necessary to accomplish demonstration and validation testing and early SA. The initial TEMP should estimate, to the degree known, the key resources necessary to accomplish DT&E, LFT&E, and OT&E. These should include the MRTFB, capabilities designated by industry and academia, and MRTFB test equipment and facilities, unique instrumentation, threat simulators, targets, and M&S. As system acquisition progresses, the preliminary test resource requirements will be reassessed and refined and subsequent TEMP updates will reflect any changed system concepts, resource requirements, or updated threat assessments. Any resource causing significant test limitations should be discussed with planned corrective action outlined. As a general rule, only address new high dollar resources, rather than a laundry list of readily available or inexpensive resources. The AST, specifically, the developmental tester and operational tester, should provide input specific to their requirements and indicate which requirements each tester identified. Specifically identify the following test resources with a table or matrix recommended for each.

a. Test articles. Identify the actual number of and time requirements for all test articles, including key support equipment and technical information required for testing in each phase by major type of DT&E and OT&E. If key subsystems (components, assemblies, subassemblies or software modules) are to be tested individually, before being tested in the final system configuration, identify each subsystem in the TEMP and the quantity required. Specifically identify when prototype, engineering development, pre-production, or production models will be used.

b. Test sites and instrumentation. Identify the specific test ranges/facilities to be used for each type of testing. Compare the requirements for test ranges/facilities dictated by the scope and content of planned testing with existing and programmed test range/facility capability, and highlight any major shortfalls, such as the inability to test under representative natural environmental conditions. Identify instrumentation that must be acquired or developed specifically to conduct the planned test program. Clearly identify the test investment requirement to ensure test site instrumentation availability and capability. Describe how environmental compliance requirements will be met.

(1) Testing will be planned and conducted to take full advantage of existing investment in DoD ranges, facilities and other resources, wherever practical.

(2) In order for the Army to realize maximum value from its capital investment in test facilities, it is necessary that PEO/PMs coordinate developmental test requirements with the AST and specifically, the developmental tester from DTC. This should be accomplished early in the acquisition cycle, preferably prior to MS B. This coordination should facilitate the development of DT requirements and determine the extent and nature of contractor services, if required. If DTC cannot conduct the DT (for example, scheduling does not permit), the PEO/PM has the authority to use contractor support. This decision and rationale will be documented in this paragraph of the TEMP.

c. Test support equipment. Identify test support equipment that must be acquired specifically to conduct the test program. Address only new test support equipment. This includes software test drivers, emulators, or diagnostics, if applicable, to support identified testing. Identify unique or special calibration requirements associated with this test support equipment.

d. Threat representation. Identify the type, number, availability, and fidelity requirements for all threat systems/simulators. Compare the requirements for threat systems/simulators with available and projected assets and their capabilities. Highlight any major shortfalls. Each representation of the threat will be subjected to validation procedures to establish and document a baseline comparison with its associated threat and to ascertain the extent of the operational and technical performance differences between the two throughout the simulator's life cycle. Threat systems/simulators to be used in activities supporting milestone decisions must be validated and accredited for the specific application. Validation and accreditation procedures are to be documented in accordance with the Army Validation and Accreditation Plan. The resulting report should be cited in annex A, the bibliography of the TEMP. For non-tactical C4/IT programs, threat representation is generally not applicable.

e. Test targets and expendables. Identify the type, number, and availability requirements for all targets, flares, chaff, sonobuoys, smoke generators, and acoustic countermeasures, that will be required for each phase of testing. Identify any major shortfalls. Include threat targets for LFT lethality testing and threat munitions for vulnerability testing. High fidelity targets require the same validation and accreditation process as for threat systems and simulators. Results of this effort should be cited in annex A, the bibliography of the TEMP. Each threat target will be tailored to characteristics of interest, in order to establish and document a baseline comparison with its associated threat and to ascertain the extent of operational and technical performance differences throughout the threat target's life cycle. Identify the schedule impacts, if any, associated with test target development. For non-tactical C4/IT programs, test targets and expendables are not applicable.

f. Operational force test support. For each T&E phase, identify the type and timing of aircraft flying hours, ship steaming days, and on-orbit satellite contacts/coverage, and other critical operating force support required. Include size, location, and type unit of unit required.

g. Simulation, models, and testbeds. For each T&E phase, identify the system simulations required, including computer-driven simulation models and hardware/software-in-the-loop testbeds. Identify the resources required to validate and accredit their usage.

(1) Include only those simulations, models, and testbeds that will be used to extend testing and/or used in the system evaluation. This includes feeder models.

(2) Simulations, models, and test beds used solely for engineering purposes (not in support of and/or used in system evaluation). This includes feeder models.

(3) Simulations, models, and test beds used solely for engineering purposes (not in support of program decisions) do not need to be identified in this paragraph.

(4) Include all hardware-in-the-loop, simulations, flight mission simulators, systems used as test prototypes, training simulators, and other test assets essential to wartime problem identification and resolution, system change T&E, and sustainment.

h. Special requirements. Discuss requirements for any significant non-instrumentation capabilities and resources such as special data processing/databases, unique mapping/charting/geodesy products, extreme physical environmental conditions or restricted/special use air/sea/landscapes. Software resource requirements are found in the computer resources life cycle management plan (CRLCMP).

i. Test and evaluation funding requirements. Estimate, by fiscal year and appropriation line number (program element), the funding required to pay direct costs of planned testing. State, by fiscal year, the funding currently appearing in those lines (program elements). Identify any major shortfalls.

j. Manpower/personnel training. Identify manpower/personnel and training requirements and limitations that affect T&E execution.

D–6. Annexes and attachments

a. Annex A—Bibliography.

(1) Cite in this section all documents referred to in the TEMP.

(2) Cite all reports documenting developmental, operational, and LFT&E.

b. Annex B—Acronyms. List and define all acronyms used in the TEMP.

c. Annex C—Points of Contact.

d. Attachment 1—Requirements/Test Crosswalk Matrix.

(1) The purpose of this annex is to provide a linkage among the AoAs, MOE, MOS, KPP, COI, and CTP, and then relate these items to specific test events for identification of data necessary to evaluate the system against the requirements. This crosswalk will consist of a foldout spreadsheet or matrix as shown in figure D–2.

(2) The linkage can be developed using any one of the categories to generate the association. Since the COI are usually the fewest in number, it may be easiest to begin with the COI and then develop the linkage with the other categories. The MOE/MOS column should reflect precisely the MOE/MOS table contained in Part I of the TEMP. The CTP column should also reflect precisely the CTP matrix in Part I of the TEMP.

COIs	AOA	MOE/MOS **KPP	CTPs	ORD (Ref Par)	EMD-DT	EMD-OT	96-98 Digitization Technical Tests	98 Digitization Customer test	CDS4 Technical Test	CDS4 Operational Test	Additional Testing
1. Is the OH-48X capable of conducting armed reconnaissance in the air cavalry unit?	Mission Performance	1) Mission Capable**	HOGE	5.c(1)a	x	x	x				
			VROC	5.c(1)b	x	x	x				
			Endurance Flight Time	5.c(1)c	x	x	x				
			HOGE at alternative MGW	5.c(1)d	x	x	x				
			Controllability	5.c(1)e	x	x	x		x	x	
			Dash airspeed	5.c(1)f	x	x	x				
			Slope landing	5.c(1)g	x	x					
			Max power rating	5.c(1)h	x	x	x				
	Target Accuracy Target Acquired	2) Visionics	Target acquisition, designation, and location	5.e	x	x	x	x	x	x	
		3)Avionics	Navigation capability	5.g(2)	x	x	x	x	x	x	
			Communications	5.g(3)	x	x	x	x	x	x	
		4) Armament		5.h	x	x	x	x	x		
	Battlefield Information	5) Interoperability **	Interoperability	DOD JTA	x	x	x	x	x	x	
		6) Countermeasures		5.i	x	x					
		7) Ballistic Protection		5.J							x
		8) NBC Survivability		5.m	x	x					
2. Can the Armed OH-48X be deployed to, and sustained in, an operational environment?	Mission/Day, Response Time	1) Transportability		5.l	x	x					
	Mission Completion Rate	2) RAM	MTBMAF	5.k(2)	x	x	x	x	x	x	
			Mission reliability (4 hr mission)	5.k(2)	x	x	x	x	x	x	
			MTTR	5.k(2)	x	x	X	x	X	x	
			MR (AVIM)	5.k(2)	x	x	X	x	X	x	
			MR (AVUM)	5.k(2)	x	x	X	x	x	x	
		3) Human Factors		5.s	x	x	x	x	x	x	
3. Can the Armed OH-48X meet mission requirements in operational electromagnetic environments? (AI)	Mission Completion (E^3) Environment	1) E3	EMI/EMV	5.u	x	x	x	x			x

Figure D–2. Sample requirements/test crosswalk matrix

(3) The second part of the matrix should consist of all test events contained in the test strategy. For each test event, an "X" is placed in a box, provided data from that test will be used to satisfy the corresponding requirement.

e. Attachment 2. Reserved for full set of COIC, to include Issue, Scope, Criteria, and Rationale.

Appendix E

Critical Operational Issues and Criteria Format and Content

E–1. Overview of critical operational issues and criteria

COIC are, by definition, those decision maker key operational concerns (issues) with bottom line standards of performance (criteria), that, if satisfied, signify that a system is operationally ready to proceed to FRP.

a. Critical operational issues are those key decision maker operational concerns that must be answered for the FRP DR to proceed. They are operationally oriented and not technology, cost, or politically focused. A typical set of COI is given below. Note that a system is considered operationally ready (effective, suitable, and survivable) to proceed to full production when the following operational concerns are answered affirmatively:

(1) Does the system satisfy the reasons for the operational requirement being established and an acquisition program initiated?

(2) Can the system accomplish its critical missions?

(3) Can the system maintain trained preparedness in peacetime for critical missions?

(4) Can the system be deployed when and where needed for critical missions?

(5) Can the system be sustained during combat and/or other critical operations? This does not mean that there are always four or five COI. These concerns may be adequately addressed in one, three, or more COI as appropriate for a system. However, COI by their nature are few in number. Additionally, programs covered by the Defense Acquisition Guidebook require a COI for interoperability. One or more concerns may be covered in the criteria or may be considered not to be applicable for the system. In the latter case, the COIC development team must be prepared to justify such determination and address it in the COIC approval submission memorandum (see app F).

b. COIC criteria are bottom line standards of performance for satisfying a COI and are showstoppers if not satisfied for the FRP DR. If a shortfall exists for one or more of the COIC criteria at the FRP DR, convincing evidence (that is, other effectiveness, sustainability, and cost data, analyses, and resulting considerations along with review of program alternatives) must be provided for the decision authority to allow the program to proceed. Like the issues, the criteria are operationally oriented and not technology, cost, or politically focused. This does not mean that the criteria are operational test oriented, just that the criteria provide operationally relevant measures. While most criteria will be answered using multiple data sources including some form of operational test, some criteria, such as NBC contamination hardening, when a specific program objective, must depend on developmental test or simulation output data. Each critical operational issue will have at least one criterion.

Note. For systems on the OSD T&E Oversight List, the DOT&E provides the statutory BLRIP report to the Secretary of Defense and Congress before the FRP DR. This report concludes whether the system is operationally effective, suitable, and survivable to enter production. If there are shortfalls in any COIC, any evidence that the system is still effective, suitable, and survivable must be provided to and considered by the DOT&E before this report is released.

c. The system of concern is the total operational system (see fig E–1) as a composite rather than any of its component parts. Simultaneously, the total system of interest may be a single system (for example, a truck with trailer) or an operational unit (for example, a team or platoon). This has several benefits, not the least of which is fewer issues. In addition, they are more relevant to operations than if focused on system components, and the potential for duplicate coverage is reduced.

d. The COIC structure (fig E–2) provides for each issue: a scope paragraph (conditions for evaluating the issue), its associated criteria, and a rationale section (basis for each criteria). Additionally, the structure provides a notes section including two standardized mandatory notes (the first addressing the total system focus and coverage of the criteria; the second addressing the pass/fail application of the COIC) and other system specific notes as needed. A third mandatory note (stating that COIC are based on initial requirements and will be updated prior to MS C) is included for COIC supporting the MS B TEMP. If this is a system for which MS C is also the FRP DR and the ORD requirements and COIC are still soft (such as require update), then a point between MS B and C should be identified for ORD, COIC and TEMP update. As the structure indicates, the criteria are the instruments for judging whether an issue is satisfied (that is, achievement of all criteria results in a satisfied issue). This structure applies to COIC coordination, approval, and processing; TEMP content; and SEP content. COIC are coordinated, staffed, and approved as a stand-alone document. Chapter 4, figures 4–8 and 4–10, provides more details on the COIC coordination and submission packages.

e. Initial COIC are developed, approved, and included in the TEMP prior to MS B. As the program progresses, they are updated as needed (particularly in response to the ORD update for MS C when a separate FRP DR is planned). The issues being based on the MNS will seldom change; however, the criteria will change as the operational

requirement matures and in response to significant program restructures (for example, shifting of pre-planned product improvements or evolutionary acquisition increments). Criteria for the COIC applicable to the TEMP at MS B may be "soft" (that is, provide a performance standard but not a final performance threshold; for example, must have high probability of accomplishing mission X). Criteria will be "firm," measurable performance thresholds for the COIC applicable to the TEMP at MS C and subsequent COIC updates. COIC updates required by program restructure/redirection between MS B and C (but not in response to the revised ORD preparatory to MS C) may continue to be "soft" if MS C is not the FRP decision for the program. These are in effect the MS B TEMP COIC.

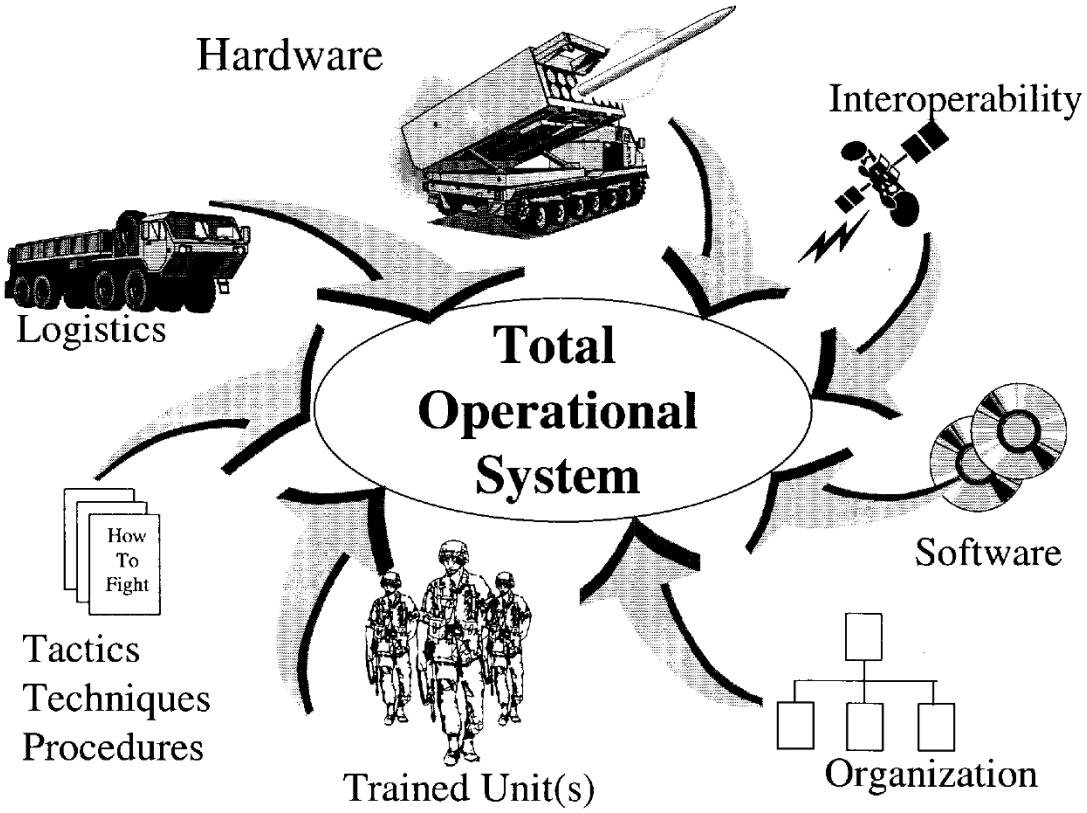


Figure E–1. Total operational system

E–2. Identifying and developing critical operational issues

a. Critical operational issues. Critical operational issues, by definition, are those key operational concerns expressed as questions that when answered completely and affirmatively signify that a system or materiel change is operationally ready to transition to FRP. They are few in number, based on the MNS, and focused on the FRP DR. There are four key components of a properly structured critical operational issue statement:

(1) *The interrogative.* An interrogative word demanding a "yes" or "no" answer (for example, "Does," "Can," or "Is").

(2) *The system.* Identification of the system of concern (for example, system X or a platoon equipped with system X).

(3) *The capability.* A capability of concern (for example, robust voice and data communication or effective aerial reconnaissance).

(4) *The conditions.* A set of applicable operational conditions (for example, during combat operations or as employed by Special Operations Forces).

b. Focus of critical operational issues.

(1) Critical operational issues focus on the total operational system as an entity and its ability to satisfy the operational capabilities defined in the MNS or Mission Needs Analysis. This focus for COIC results in a few issues that seldom change as the system progresses through the acquisition process. While the norm is four issues (one for mission

accomplishment, one for deployability/mobility/survivability, one for interoperability, and one for sustainability), as few as one (single shot item or system change) or as many as six (a family of trucks) may be appropriate. This focus breaks the mindset of separate operational effectiveness and suitability issues. A single issue will often cover the areas of mission performance, survivability, RAM, MANPRINT, and software performance (for example, probability of successful communications for a communications net or probability of find and kill targets entering a system's (could be an organization equipped with the new system) area of influence for a direct fire weapon).

Critical Operational Issues and Criteria
for
the "X" System, System "X" Block "Z", or "Y" Modification to the "X" System)
for Test and Evaluation Master Plan Supporting
Milestone B or C, FRP Decision, Modification Approval Package, or other event

1.0 Issue: (see para E-2.)
1.1 Scope: (see para E-3.)
1.2 Criteria: (see para E-4.)
1.2.1 **A dendritc numbering system is used to standardize format.**
1.2.2
1.2.*n*
1.3 Rationale: (see para E-5.)
1.3.1 **Rationale subparagraphs correspond to those of each criterion.**
1.3.2
1.3.*n*

2.0 Issue: **Subsequent issue sets are numbered 2 through n.**

Note: The total issue sets is normally three or four and 9 to 12 criteria. As few as 1 issue set with 7 criteria (for example, single shot item) or as many as 7 issue sets with 20 criteria (for example, a truck family) may be right for a given system. Key is identifying and defining only the "show stoppers" for the good enough system.

Note 1: (mandatory) (see para E-6b.)
Note 2: (mandatory) (see para E-6c.)
Note 3: (mandatory for MS B TEMP COIC) (see para E-6d.)
Notes 4: through n: (system peculiar -- see para E-6e.)

Figure E–2. Critical operational issues and criteria structure

(2) Operational relevancy translates as "accomplish critical missions," "maintain trained preparedness for operations," "can be deployed when and where needed," and "can be sustained at operational tempo during operations." "Accomplish critical missions" means not only that the system is capable of performing its mission functions, but is reliable and survivable to the degree needed during the mission; and can interoperate with Army, Allied, and other-Service systems necessary for mission success. "Maintain trained preparedness for operating" assesses the ability of units to train in garrison to be mission ready with the system. This is not limited to training and retaining skills for OT, but looks to the fielded system, its training program, and the Soldiers who will lead, operate, and sustain the system. "Can be deployed when and where needed" includes not only movement to the theater of operation but movement within the theater, set-up, and placement into operation. "Can be sustained in combat" assesses the impact of the systems logistics footprint on the employing and sustaining units, when operating at operational tempo, particularly during early employment operations until a large-scale logistics build-up is achieved and/or sustained high intensity operations when a large-scale logistics build-up is achieved.

c. Mission accomplishment issue. From the view of minimizing the COI, preparation of the COI starts with the mission accomplishment issue. Normally a good procedure is to frame the critical mission/task order to be given by higher headquarters as the issue (for example, "Can the unit equipped with system X take and hold the tactical objective on the future battlefield?" or "Can truck X pick up and transport required tactical loads to objective location as required in support of combat operations?"). Next, complete the issue with its scope, criteria, and rationale. Then, if there is anything remaining unaddressed in the mission accomplishment area, define that issue with its scope, criteria, and rationale, remaining cognizant of the first issue and criteria to avoid duplication or overlapping coverage. Once the mission area is complete, consider the need for a sustainment issue. If a sustainment issue is not needed, provide the rationale in your cover memorandum when coordinating the COIC and when submitting the COIC for approval. Once the set of COIC is complete, review it for duplication or overlapping coverage, and eliminate any redundant issues.

Note. Interoperability COI is mandatory for all programs on the OSD T&E Oversight List. The Defense Acquisition Guidebook encourages that those programs have a COI for interoperability in the TEMP. The Joint Staff is to ensure system requirement documents (CRDs and ORDs) contain operational interoperability required capabilities and KPP to support development of criteria for this COI.

d. Questions to ask when developing the critical operation issue.

(1) What is the system of interest? For example: individual system (tank round, rifle, and so forth), system of systems (communications network/air defense platoon/information management system), or system component change (improved missile warhead).

(2) Why the system (or system change)? For example: the deficiency the system is being designed to correct or opportunity it is intended to seize.

(3) What are the critical missions? To determine, consider all missions against the question, "Which mission requirements, if not satisfied, will engender a "No-Buy" decision," where there is more than one but similar critical missions, "Which mission is the more rigorous/demanding," and where there is more than one, but distinctly dissimilar critical missions.

(4) Are there critical user, unit concerns? For example, "Is the system deployable by light forces?"—if not, "Is a "No-Buy" decision in order?"

(5) What are concerns regarding sustainment? For example, "Is the Ammunition Supply Point throughput capacity sufficient to support a significantly higher rate of fire capability for a cannon artillery system?"

e. Do and do nots when developing the critical operational issue.

Note. Each "Do" is followed when appropriate by one or more companion "Do Nots."

(1) *Focus.* Do focus the issue so as to properly direct the evaluation and decision. State a question that asks if a task can be performed under the conditions of concern (for example, "Does the Nipper effectively close with, detect, engage, and destroy threat armor under expected battlefield conditions?").

(a) Do not over generalize (for example, "Is the Nipper operationally effective?" or "Is the Nipper operationally suitable?").

(b) Do not include criteria in the issue statement (for example, "Does the Nipper find and kill X percent of threat armor within its area of operations?").

(2) *Decision issue.* Do formulate the issue as a question that demands a "yes" or "no" answer (a decision). Begin the question with words such as "Can," "Does," or "Is" (for example, "Can the Nipper equipped units achieve and maintain a level of training readiness during peacetime and provide for a wartime readiness capability for sustained combat operations?"). Do not formulate the issue as an investigative question that demands an analytical answer by beginning the question with words such as "How well" or "What is." For example, do not contrast "How well does the Nipper close with, detect, engage?"

Note. An investigative issue may be appropriate for an evaluation focus area (that is, AI) since their focus is the evaluation and not the decision.

(3) *Minimize issues.* Do limit to a few issues by focusing on the total system need and concerns for the FRP DR.

(a) Do not duplicate coverage by overlapping issues (without good reason).

(b) Do not get bogged down in the "eaches" of a system (for example, elements of operational effectiveness/suitability and ORD operational characteristics).

(4) *Apply experiences.* Do use COIC approval successes as a guide, not as a rule. Apply experiences during recent COIC approval actions while recognizing system differences. Seek out COIC examples that have been processed

recently and are at the same approval level as the set being developed. Talk to those involved in the processing of the COIC example about their experiences and any special considerations that may have affected their COIC approval.

E–3. Identifying and defining the scope in critical operational issues and criteria

a. Identifying and defining. The scope, by definition, is a statement of the operational capabilities, definitions, and conditions that focus each issue and its evaluation. There will be a separate scope statement for each issue even though the scope for the second or successive issues may refer to and expand upon the scope statement for issue one. The scope normally begins with the words, "This issue examines...," and identifies—

(1) *Capabilities.* Operational capabilities to be examined (for example, mission accomplishment, sustainment training, and/or combat sustainment).

(2) *Definitions.* Special terms, either system peculiar requiring definition (for example, system description, grade of service, communication connectivity, or vehicle payload) or measurement peculiar (for example, start/stop points for time measures).

(3) *Conditions.* Evaluation conditions including tactical context and scenario (for example, the OMS/MP or the Southwest Asia standard scenario); force structure and deployment considerations (for example, D&O TSP and Corps/Division/Other slice); approved threat (for example, threat TSP and STAR); crew and maintainer descriptions; and environmental conditions (for example, natural and dirty battlefield).

(4) *Other data sources.* When an issue and any of its criteria require technical test or modeling/analysis support.

b. Questions to ask when developing the scope of critical operational issues and criteria.

(1) What are the operational capabilities of concern?

(2) Do force-on-force operations apply, and if so at what level (for example, EW only or armored force in accordance with approved threat package and scenario)?

(3) What friendly force structure and operations are necessary (for example, single system only or force slice; crew and maintainers; or approved OMS/MP and scenario or only elements thereof)?

(4) What environments apply? (for example, natural ones—terrain, visibility, day/night, climate—and battlefield MOPP level, obscurant, electronic countermeasures, and so forth).

(5) What terms need definition (for example, those that are system, operation, and measurement peculiar)?

(6) Do any special evaluation methods apply (for example, technical test or application of analytical means)?

c. Do and do nots when developing the scope of critical operational issues and criteria.

(1) *Focus issue.* Do focus evaluation of the issue by identifying operational capabilities of concern, applicable operational conditions, applicable definitions, and special evaluation methodologies (that is, when technical test, simulation, or other analytical means are used in lieu of or to supplement OT).

(a) Do not specify criteria (that is, characteristics with performance standards).

(b) Do not specify rationale (that is, justify the issue or criteria).

(c) Do not include specific conditions/definitions better suited as part of the criteria (for example, detection/engagement envelope, line of sight, pallet weight for upload, and so forth).

(2) *Development procedure.* Do initially prepare the scope in draft and finalize only after developing applicable criteria (that is, selection of specific criteria may in fact necessitate unique conditions, definitions, or evaluation methodologies not initially anticipated).

E–4. Identifying and developing the criteria in critical operational issues and criteria

a. Criteria in critical operational issues and criteria. Criteria are, by definition, those MOPs that when achieved signify that the issue has been satisfied and the system should move forward to the FRP DR. Criteria will be few in number, but there will be at least one criterion for each critical operational issue. Criteria will—

(1) *Be focused.* Criteria focus on the total operational system and on providing operational performance standards for the FRP DR, even though they may be "soft" when initially developed and included in the MS B TEMP (for example, "Will be capable of killing tank X" versus "Will have a 50 percent chance of finding and killing tank X without becoming targeted by threat weapons."). When "firm" criteria are known early, they will be stated (for example, "Will be mission capable roll-on, roll-off transportable by C–130 aircraft.").

(2) *Reflect system maturity.* Criteria are formulated without losing sight of the fact that the "system" is in a constant state of development (for example, even a non-developmental item frequently does not have mature TTP, training, and logistics at the FRP DR).

(3) *Be "showstoppers."* Criteria are formulated to reflect showstopper measures (for example, if all criteria are met, the system is operationally good enough; or, to the contrary, if a criterion is not met, the FRP decision should not be given). Mandatory note #2 is provided to avoid use of criteria as automatic pass/fail measures during evaluation

and decision making. Other credible evidence of an operationally effective and suitable system when available will be considered to arrive at the proper decision.

(4) *Be traceable to the operational requirements document and analysis of alternatives.* This does not mean that criteria are to be direct lift from these documents, but that they are traceable by rationale to specific requirements and findings of these documents. In the case of ORD KPP, they are to be direct lifts from the ORD to the COIC criteria statement. Other criteria statements may be developed by combining two or more requirements into a single higher order of measure, or drawn from sources other than the requirement (like the AoA) to provide specific MOPs not provided in the requirement document (for special emphasis, when applicable, must be devoted to choosing which type of total system (individual or unit) is to be examined and whether the characteristic of interest is a performance standard or a baseline comparison. Additionally, the following must be considered: criteria mature with the operational requirement ("soft" for MS B TEMP and "firm" for MS C TEMP); the system (hardware, software, and TTP) example, the ORD requires improved survivability whereas cost and AoA data support a need for 20 percent more combat capable systems).

b. Criterion statement considerations.

(1) *Criterion statement components.* Figure E–3 depicts the major elements of a criterion statement, each of which must be addressed, and presents an example of a properly constructed criterion statement with explanations for the specific wording. Special emphasis, when applicable, must be devoted to choosing which type of total system (individual or unit) is to be examined and whether the characteristic of interest is a performance standard or a baseline comparison. Additionally, the following must be considered: criteria mature with the operational requirement ("soft" for MS B TEMP and "firm" for MS C TEMP); the system (hardware, software, and TTP) is still maturing at the FRP DR; information available from the requirement document (lack of specificity in performance parameters may increase the potential for evaluation bias and thereby dictate use of baseline comparison); and the acquisition objective (cost may override performance and the criteria therefore reflect current system performance). As reflected in figure E–3, there are choices for each element wherein the correct choice is system/situation dependent (for example, a tank and a communications system will have differently structured criteria). As a criteria structure illustration, consider the criterion statement, "The tank will kill at least 50 percent more enemy armored vehicles at ranges out to three kilometers." The object to be examined is "the tank." The characteristic of interest is "kill armored vehicles," which constitutes a critical performance capability, and the qualifier "more" alludes to a comparison with a baseline. The magnitude of 50 percent is quantitative and the direction "at least." The constraint condition of "out to three kilometers" is both operational and tight, and "enemy" implies battlefield conditions. The scoring criterion is "kill," which would be based on definitions (mobility, firepower, catastrophic, and so forth).

Note. A caution on constraint conditions—they must be operationally realistic. If, for example, their interpretation allows for use of unrepresentative threat or friendly operations in T&E, they have been improperly stated.

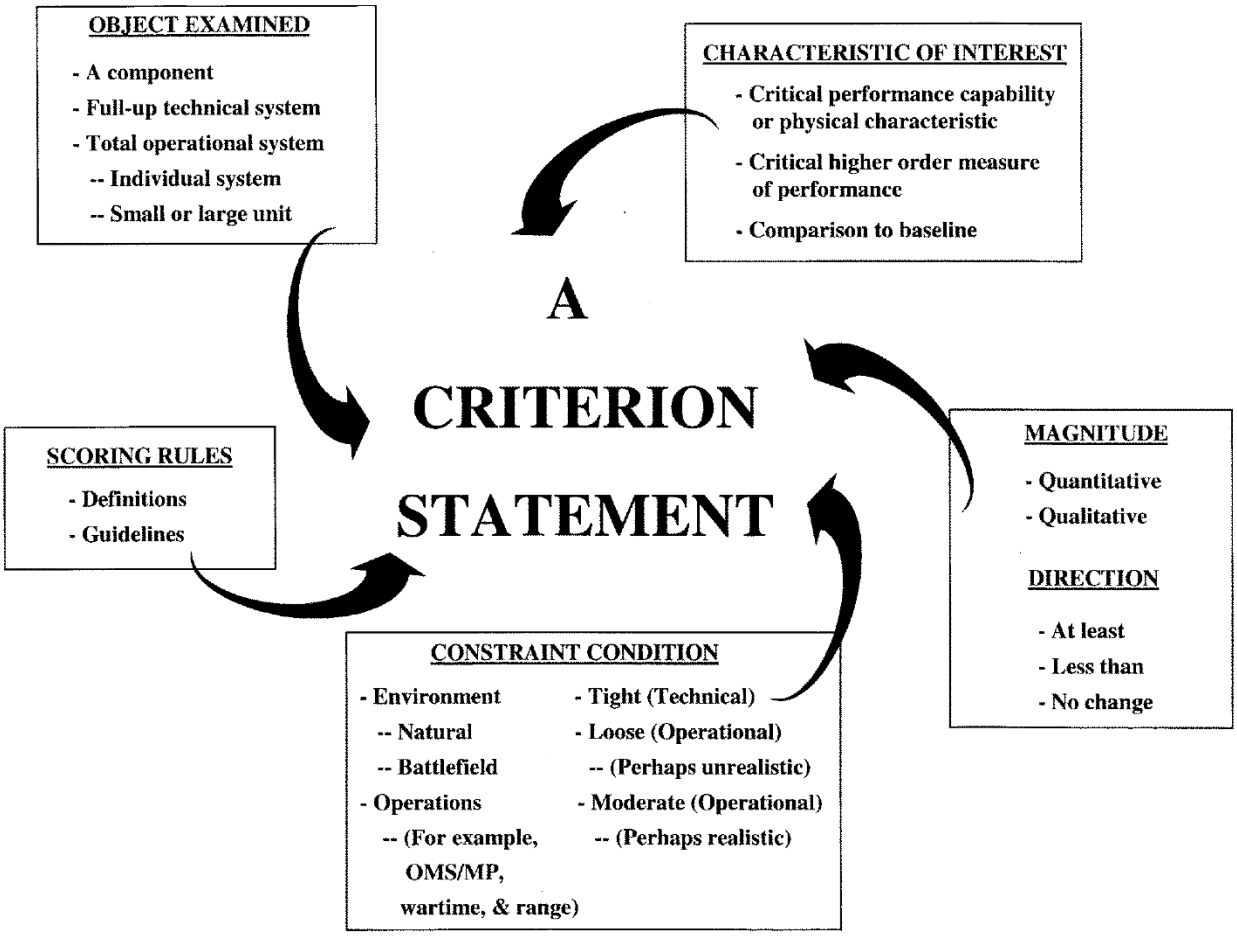


Figure E–3. Major elements of a criterion statement

(2) *Individual system versus organizational unit.* As indicated earlier, special emphasis must be placed on choosing the correct total system—an individual system or an organizational unit—to be the object examined (see fig E–4). Factors that would lead to selection of a single system include technical criteria (for example, ascend/descend a 60 degree concrete slope); the system operates and/or is employed as an independent system (tractor and trailer); or the purpose of the acquisition is to benefit the system alone (for example, larger caliber tank main gun). Factors which would lead to selection of an organizational unit include the acquisition is to benefit a unit (for example, an automatic detection and defense system authorized, one to a platoon to improve platoon survivability and operations); the system operates and/or is employed as an element of a unit (for example, an air defense system—fire unit—which operates as a team member providing and receiving target detections, cueings, hand-offs, and engagements to and from other fire units in the platoon); the system represents a system of systems (for example, a force level communications system made up of multiple, dissimilar subsystems); or a concern (characteristic of interest) which requires a unit to measure (for example, more combat capable vehicles remaining). When an organizational unit measure is chosen, the measure must assess the contribution of the system to the unit mission. When multiple systems are present in an organizational unit, some force measures mask the contribution (or lack there of) to unit mission. Force effective measures such as loss exchange ratios should only be used when the force is composed of a single system in acquisition and when M&S is part of the evaluation to expand beyond actual test trials. Within a set of COIC, both system and organizational unit measures may be used.

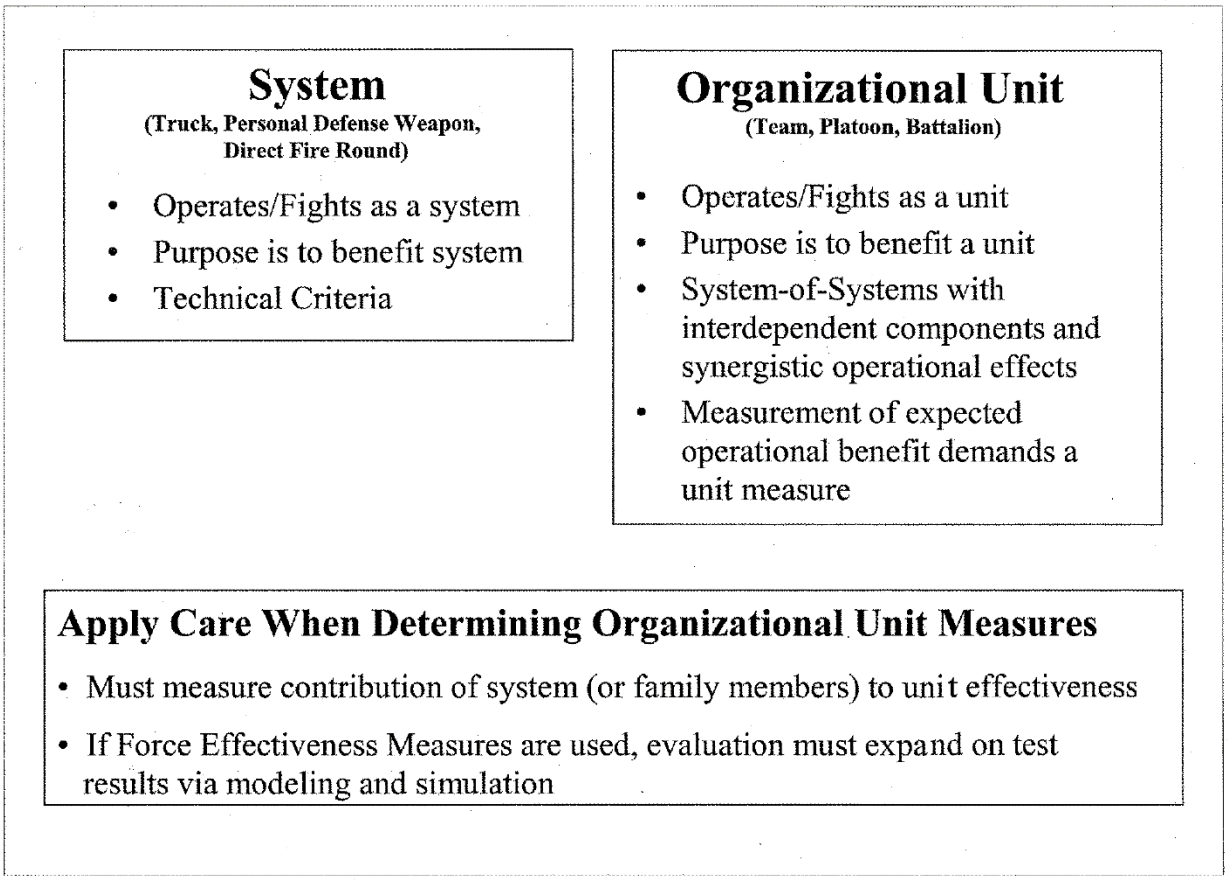


Figure E–4. System versus organizational unit measure

(3) *Performance standard versus baseline comparison criteria.* Also, as indicated above, special emphasis must be placed on determining whether the characteristic of interest can be stated as a performance standard or will require baseline comparison. Most characteristics of interest will be stated as performance standards. However, two key situations will dictate use of baseline comparison: the system is a replacement system or a system change to an existing system and the requirements documents or other sources fail to provide an adequate basis for deriving performance standards; or, the independent system evaluator identifies and justifies, to the satisfaction of the CBTDEV or FP, that there is sufficient risk of bias in T&E. Although this is a break with the past when baseline comparison was reserved for exceptional cases and then only when absolutely necessary, baseline comparison is now encouraged in the situations outlined. It should be kept in mind, however, that the use of baseline comparison criteria results in side-by-side comparison testing to support evaluation of the system. The criticality of this approach to the evaluation effort must therefore be sufficiently high to justify the expenditure of significant additional resources. Another caution is that a baseline comparison may also mask achievement (or non-achievement) of a new key capability that drove the operational requirements and acquisition processes (for example, the new system can be better than the current system but still not accomplish the critical missions).

(4) *Example measures.* Figures E–5 and E–6 present additional system/situation examples of characteristics of interest and typical means of measurement. They are not complete criteria statements.

c. Do and do nots when developing the criteria in critical operational issues and criteria.

(1) *Minimum need.* Do focus on the minimum needed for the FRP DR—discard or revise if a shortfall would not be a "showstopper."

(a) Do not include "desired" characteristics.

(b) Do not specify "firm" criteria for the MS B TEMP unless known to be stable (for example, transportable by CH–47).

(c) Do not embed peripheral issues in criteria to ensure evaluation (for example, the training program must be the optimum training strategy).

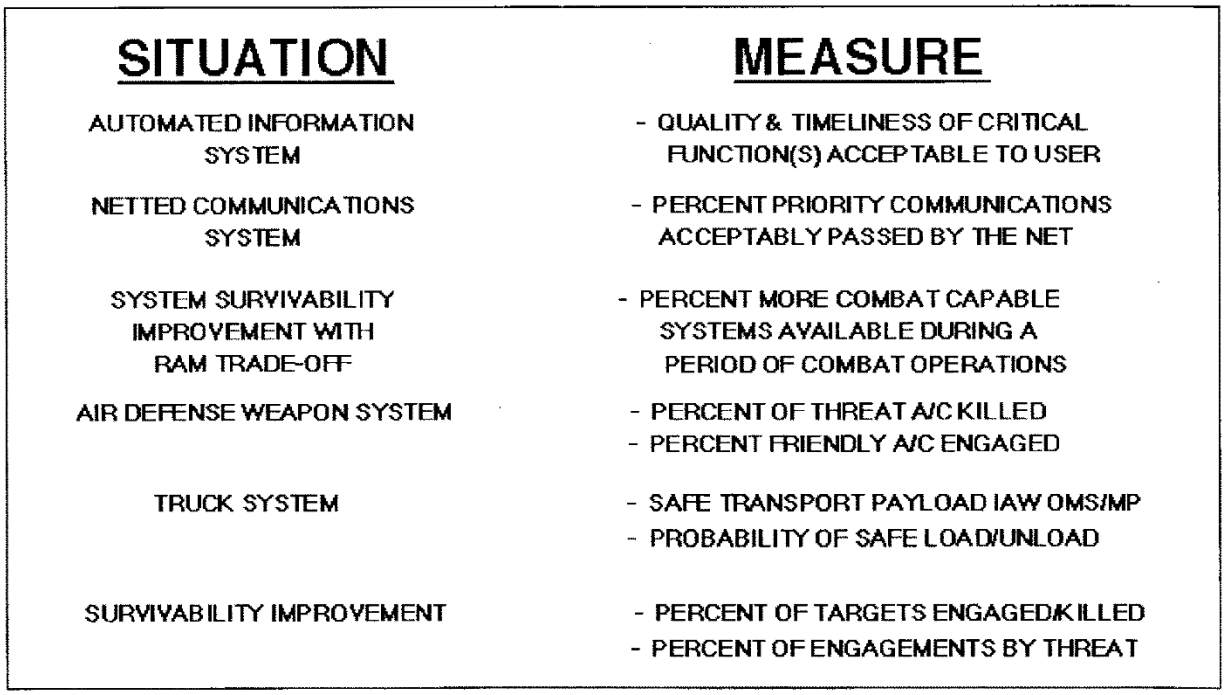


Figure E–5. Characteristics of interest—mission accomplishment examples

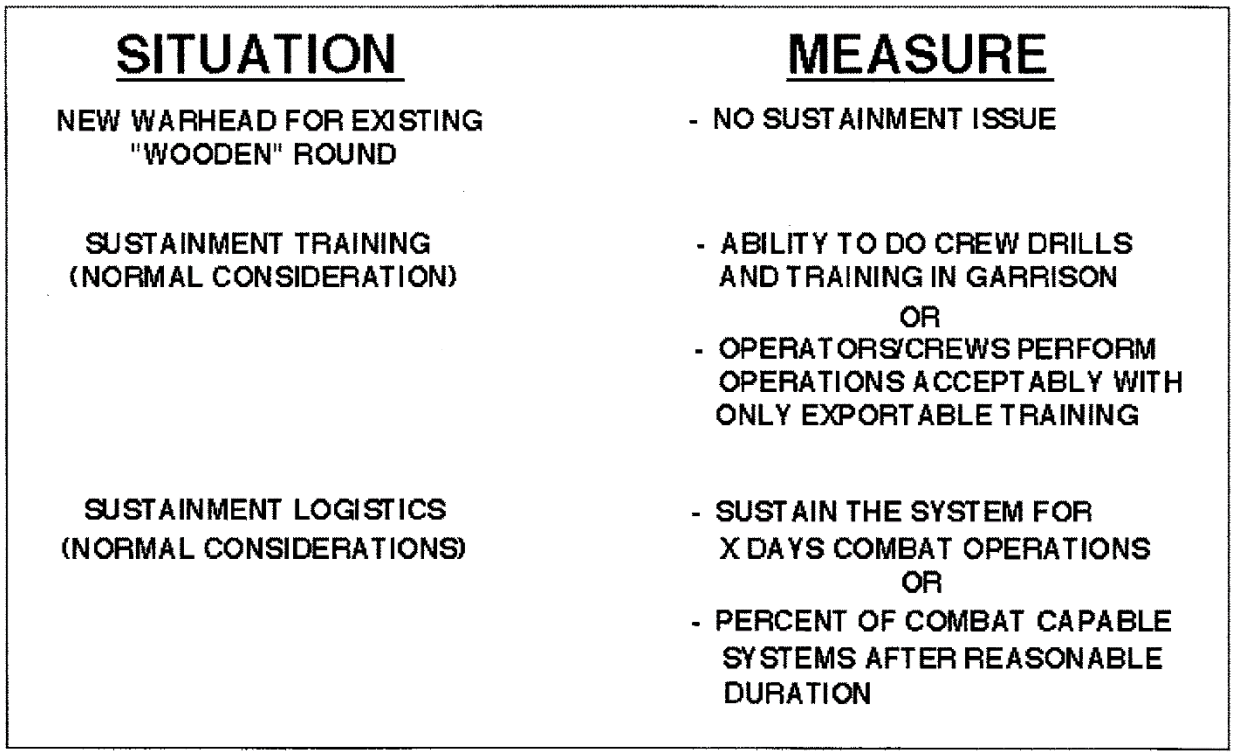


Figure E–6. Characteristics of interest—sustainment examples

(2) *Measures of performance.* Do use MOPs that emphasize the system's operational effectiveness and suitability in terms of critical combat missions to be accomplished. Do not use MOEs such as force exchange ratio, loss exchange ratio, or other such force level AoA measures that depend on large-scale modeling that is beyond the capability of the system evaluation. Operational tests do not normally provide enough trials or steady state operations to revisit the AoA.

(3) *Qualitative criteria.* Do specify qualitative criteria (which must be measurable) only when quantitative criteria are not applicable. Do not specify a confidence level. Statistical confidence levels are test resource drivers and better left to the tester and evaluator.

(4) *Test and evaluation limitation.* Do specify measures unconstrained by consideration of the applicable test/evaluation methodology to be used for resolution, if the characteristic is known to be critical and achievable. Accordingly, it will become an issue requiring resolution/adjudication above the COIC development team.

(a) Do not exclude a critical criterion because it can only be answered by technical test or simulation (criteria focus the operational evaluation and the decision, not a particular test).

(b) Do not compromise criteria to accommodate T&E frailties (that is, T&E instrumentation, facilities, or other resources should not restrict the criteria if it is deemed critical). Tester and evaluator must find methods to provide the answer if at all possible. It may be that such criteria need to apply to later increments when technology provides for the new capability.

(5) *Probabilistic measures.* Do specify Soldier-machine measures in terms of a medium value if a high degree of performance is not needed at IOC or 80/90 percent if a high degree of confidence is needed at IOC. This approach allows for improvement before IOC. Do not specify or imply 100 percent performance when the operation must be accomplished by Soldiers. The term imply includes an absolute statement of capability (for example, crews will always initialize the system and achieve operational status within 30 minutes). Such a criterion needs an associated confidence statement. Changing operational circumstances tend to compromise crew 100 percent performance.

(6) *Conditions and definitions.* Do specify the conditions and definitions needed for evaluation (for example, the operational constraint (engagement envelope) and/or scoring criteria (stop/start point for a timeline, destroy/kill definition, and so forth)). Do not leave ambiguities that can result in erroneous T&E of the criteria (for example, don't say "more survivable" because survivability can be measured as either more combat vehicles remaining at a given

point in time, or as more threat kills because the vehicle remains combat capable longer). Do not over specify constraints and definitions (for example, a constraint allowing operation only in temperatures above 70 degrees Fahrenheit would not support world-wide basic environment deployment).

(7) *Total system measures.* Do specify total system measures (for example, operator load vehicle, accomplish OMS/MP at stated speeds, C–130 roll-on/off, and so forth). Don't specify component measures (for example, materiel/software performance, human factors constraints, technical standards, and so forth).

(8) *Lowest level system.* Do specify the lowest level system possible and appropriate (the preference is a single system but, when required, an organizational level may be more appropriate) (for example, a howitzer product improvement program (PIP) used the individual howitzer for mission accomplishment and the battalion for battlefield availability (a measure that addresses survivability and operational readiness); communications systems normally use nets for mission accomplishment and key components for set-up/tear-down time; trucks are typically assessed with trailers, and so forth). Do not measure a structure that obscures performance of the system of concern (for example, a major performance improvement to vehicle type in a fleet may provide significant improvement in overall platoon operations and only slight improvement in some combined arms team measures).

(9) *Higher order measures.* Do specify higher order measures (for example, percent target kill, percent messages sent and received, and so forth). Do not specify "eaches" (for example, probabilities of detection, identification, handoff, engagement, hit, and kill given a hit for a weapon; probabilities of connectivity, message receipt given connectivity and being available for a communications system, and so forth).

(10) *Baseline comparison.* Do specify baseline comparison criteria only when appropriate (see para E–4*b*(3)) and state an improvement percentage when the acquisition objective is improved performance and the end result will be higher system cost. Do not state an improvement percentage for baseline comparison when cost benefit is the reason for the acquisition. Do not use statistical significance as rationale for the stated improvement percentage.

(11) *Quantitative criteria.* Do use quantitative criteria, which are preferred when possible. Do not use qualitative criteria unless quantitative criteria cannot be developed or are not applicable.

(12) *"Lessons learned" (recent experiences).* Do apply "lessons learned" from previous evaluations to avoid pitfalls. Do not allow duplicate or overlapping criteria unless absolutely necessary (that is, a system should not be placed in double jeopardy for a single shortcoming).

E–5. Identifying and developing the rationale in critical operational issues and criteria

a. The rationale. The rationale, by definition, provides justification for the criteria, not the issue, and an audit trail to the requirements specified in the MNS, ORD, AoA, and system specification. It states the reason for selecting a particular characteristic or capability and identifies by document and paragraph the source of the information. In the case of derived criteria, the rationale will provide the basis and methodology used. Considering the operational nature of COIC, the rationale for the requirements is often as important as the requirement in establishing and justifying the criteria. The rationale should not be separated from the COIC since understanding the basis for a criterion is critical during its evaluation.

b. Questions to ask when developing the rationale for COIC.

(1) *References.* Are appropriate source references included for all criteria? Is there one or more ORD paragraphs referenced for each criterion stated?

(2) *Derived criteria.* Are the basis and methodology discussed for all "derived" criteria (for example, probability of kill incorporates probabilities of detection, identification, engagement, hit, and kill given a hit)?

(3) *AoA relationship.* Is the relationship between the criteria and AoA results addressed where applicable (for example, the ORD requires improved survivability (that is, over that of the baseline system) and the AoA identifies a minimum requirement for 20 percent more combat capable systems (for example, survivability and reliability trade off) to make the program the preferred alternative)?

c. Do and do nots in developing the rationale.

(1) *Criteria justified.* Do provide a complete justification for each criteria.

(a) Do not justify the issue.

(b) Do not inject new/additional criteria into the rationale.

(2) *Criteria audit trail.* Do establish a complete audit trail by indicating the specific document and paragraph within the document from which each criterion was derived or extracted. Every criterion must have a basis in the ORD. This does not mean that it must be a direct lift.

(3) *Criteria to analysis of alternatives linkage.* Do provide a defined relationship between COIC and AoA MOE/MOP whenever possible such that the system evaluator can evaluate AoA impacts should there be shortfalls against COIC.

(4) *Critical mission justification.* Do justify why a particular mission or use was selected when multiple missions or uses are possible.

E–6. Identifying and developing the notes in critical operational issues and criteria

a. Use of notes. Mandatory notes and any other required notes, explanations, or definitions will be included after the last issue set. They serve to emphasize the purpose and scope of COIC in relation to the full set of evaluation focus area measures; place T&E results related to COIC in the proper perspective; and discuss lengthy T&E conditions or definitions.

b. Mandatory note #1.

(1) *The note.* Note used to reflect appropriate characteristics applicable for the specific system (for example, if a maintenance ratio is included as a criterion, then RAM may not apply to this note): "Note #1. Criteria X, Y, and Z are total system measures. As such, they inherently cover hardware, software, personnel, doctrine, organization, and training. System individual characteristics of operational capability, survivability, RAM, organization, doctrine, tactics, logistics support, training, and MANPRINT (which includes the domains of manpower, personnel, training, HFE, system safety, health hazards, and Soldier survivability) related to these criteria will be provided by the system evaluator in the SEP."

(2) *Discussion of note #1.* This note serves to emphasize to the COIC developer that total operational system measures are preferred. This note acknowledges that some criteria will not be total operational system measures, and identifies for the evaluator and reviewers those designated criteria (X, Y, and Z) that are in fact total operational system measures. This note commits to addressing the more detailed system individual characteristics in the SEP.

c. Mandatory note #2.

(1) *The note.* Provide the following note: "Note #2. Criteria are not provided as automatic (default) pass/fail measures. Rather they represent estimates of performance for which a breach would require a careful senior level management reassessment of cost effectiveness and program options during the program milestone decision review."

(2) *Discussion of note #2.* This note emphasizes that criteria are not "automatic" pass/fail measures. This note highlights the fact that breach of a criterion constitutes a showstopper until convincing evidence can be presented to decision makers that the program should proceed in spite of the shortfall. Convincing evidence might include a revised risk assessment, specific observations and data from operational tests, baseline comparison data, AoA updates, or a revised threat assessment.

d. Mandatory note #3.

(1) *The note.* Provide the following note when COIC applicable to the MS B TEMP and the FRP DR are separate from MS C: "Note #3. These COIC are derived from the user's initial requirements for the system. These COIC will be updated prior to MS C based on the revised ORD and final updated AoA."

(2) *Discussion of note #3.* This note is applicable only for COIC in support of the TEMP approved in advance of MS B. This note highlights the fact that COIC for the MS B TEMP may contain "soft" criteria that will be updated as the system matures. Note #3 applies to COIC when "soft" criteria are used in support of the initial TEMP required for program initiation. The intent is to update the COIC and TEMP before testing/other data gathering events in support of the system evaluation required for the DRP DR. When an evolutionary acquisition is pursued, a similar note would apply for each future increment having "soft" criteria.

e. Other notes. System peculiar notes are those necessary for understanding. They will commonly focus on definitions or lengthy T&E conditions.

Appendix F

Critical Operational Issues and Criteria Process Guide

F–1. Overview of critical operational issues and criteria

This appendix provides detailed COIC process guidelines for materiel and tactical C4I/IT programs (para F–2) and non-tactical C4/IT programs (para F–3); schedule synchronization considerations for ORD, COIC, and TEMP (para F–4); and sample COIC submission and staffing memoranda (para F–5).

F–2. Materiel and tactical C4I/IT programs

Figure F–1 depicts the COIC approval process for materiel and tactical C4I/IT programs.

a. The CBTDEV has the lead for ORD and COIC development and approval processes. The CBTDEV initiates development of the ORD in response to an identified and approved materiel need from the Mission Needs Analysis, a JROC-approved MNS for ACAT I programs, and a DCS, G–3 memorandum responding to the CBTDEV's memorandum request authorization to begin preparing the ORD. The CBTDEV initiates COIC development by forming a team with the MATDEV or PM and system evaluator as an adjunct to the ICT developing and writing the ORD (see para 4–1*g*). COIC are based on ORD and the analyses supporting the ORD development. Separate COIC and ORD developments create extra work for the CBTDEV, MATDEV or PM, and system evaluator either by revisiting analyses supporting ORD development to develop the COIC or by initiating changes to an approved ORD identified during COIC development. ORD and COIC development are complementary tasks and, when properly executed, much of the COIC content may be lifted directly from the ORD. The ORD will normally lead the COIC during development process. As the ORD enters core staffing, the team will finalize the initial draft COIC (or draft revision to the COIC in the case of a change or update to an approved ORD) for coordination. COIC will not be approved until the ORD is approved because of the COIC interrelationship with and dependence on the ORD. Any change in an approved ORD KPP will normally require a change in the COIC, since KPP are extracted verbatim from the ORD for inclusion in COIC. Change in other approved ORD required capabilities or constraints may require a change in COIC. A change to previously approved COIC may require an ORD change.

b. Per figure 4–8, the draft COIC are readied for and begin coordination while the ORD is in core staffing. While the CBTDEV has the lead for the product being coordinated, it is a team effort with the MATDEV or PM and system evaluator who also have a vested interest and must participate in the process and consider comments received. The MACOM provides comments and advice reflecting consideration of emerging MACOM operational/warfighting concepts as well as cross-MACOM experiences with requirements and COIC approval and application during acquisition. The T&E WIPT provides comments and advice concerning ability to answer the COIC (for example, methodologies available or needed, program resource implications, and risks of obtaining an erroneous answer) and proposed alternatives when applicable. The AoA report provides the analytical evidence, comments, and recommendations that will facilitate further development of the ORD and refinement of KPPs as well as how M&S may be used in supporting the evaluation of COIC. The CBTDEV, MATDEV, and system evaluator use these comments along with the ORD changes from the core staffing to refine the draft COIC. Disagreements that are irresolvable are raised through command channels for resolution. DCS, G–8 will adjudicate all irresolvable COIC disagreements. The refined draft COIC are provided to the T&E WIPT for use in the draft TEMP and to the MACOM headquarters for information and comment, as appropriate. If this should result in further change to the draft COIC, the revised draft will be provided to the T&E WIPT for inclusion in the draft TEMP and the MACOM headquarters.

c. COIC are based on the ORD. Therefore, changes that occur to the ORD during its approval process must be reviewed for impact on the draft COIC. When an ORD change impacts the COIC, the needed refinement must be made to the draft COIC. The CBTDEV, MATDEV, and system evaluator will participate and agree with the revisions. Copies of the revisions will be provided the T&E WIPT and MACOM headquarters.

d. The team agreement or identified areas of disagreement elevated to their leadership for resolution is key throughout the process. As the draft COIC are readied for entry into the approval process, these areas of agreement or disagreement are formalized for resolution in the approval process. Preference is that the ORD approval process for ACAT I/IA programs occurs before entry of COIC into the approval process, although it is recognized that this is not always possible considering time demands of milestone decision points, TEMP approval schedules, and ORD approval processes. COIC approval will not proceed beyond the MACOM headquarters until the ORD is HQDA approved. The CBTDEV has the lead for development of the COIC and is responsible for the operational relevance of the COIC and for the non-materiel DOTMLPF components supporting system's achievement of the COIC. The PM or MATDEV may (and should) nonconcur with the draft COIC if the current state of technology or planned program cannot deliver materiel (for example, hardware, software, and logistics) capable of satisfying the COIC by the FRP DR. Likewise,

the system evaluator may (and should) nonconcur with the draft COIC if any of the COIC cannot be evaluated and answered for the FRP DR.

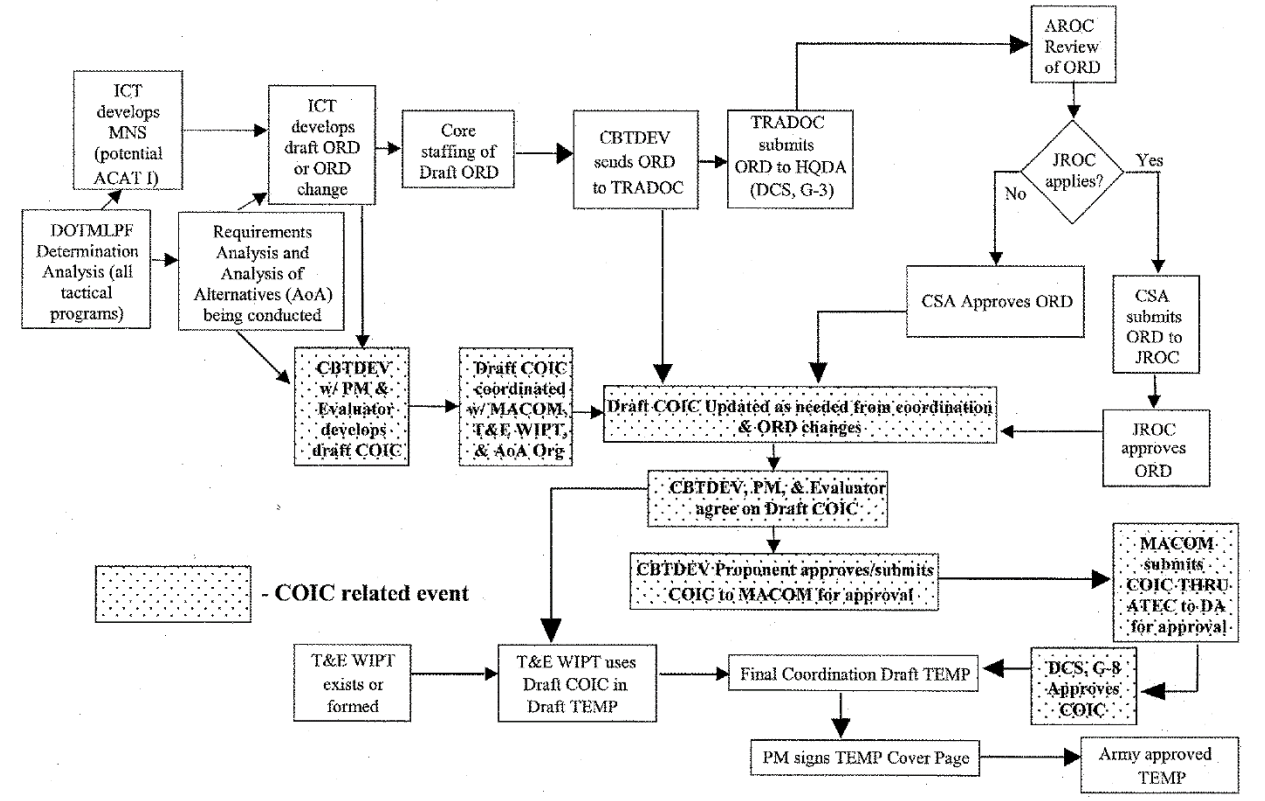


Figure F–1. Critical operational issues and criteria process for materiel and tactical C4I/IT programs

e. HQDA retains approval authority for COIC. MACOM headquarters must submit the COIC to DCS, G–8 for approval. HQDA (that is, the Army Chief of Staff, Army Requirements Oversight Council (AROC), or DCS, G–3) must have approved the ORD, including the ORD, before the CBTDEV/proponent or MACOM submits the COIC for approval. ORD–COIC crosswalk matrix (see fig F–2) must be included when the COIC are submitted for approval. While paper copies will document official submission; electronic copies serve to expedite approval processing. As a minimum, official concurrence must be provided by the MATDEV or PM and ATEC (may be by email or fax) with the proposed COIC before the MACOM submits the COIC for approval. An unresolved COIC nonconcurrence by either the MATDEV or PM or ATEC will require resolution at the MACOM headquarters level or, in exceptional cases, the DCS, G–8 level, before approval of the COIC. See paragraph 4–5*c* for the COIC submission package guidance.

f. Upon receipt of program COIC for approval processing from one of its CBTDEV schools, commands, or other organizations, the MACOM headquarters will take the following actions:

(1) Determine status of ORD approval. The ORD must be HQDA approved before MACOM headquarters forwards the COIC to HQDA for approval.

(2) Coordinate COIC with MATDEV or PM and ATEC. There should be no surprises at the MACOM headquarters, MATDEV or PM, or ATEC when the COIC arrive since previous coordination by the CBTDEV, MATDEV or PM, and system evaluator with their leadership should have already occurred. Therefore, the MATDEV or PM and ATEC command positions should be received within 15 calendar days. If this is not the case and the proposed COIC represent a surprise to the MACOM headquarters, MATDEV or PM or ATEC, the MACOM headquarters will determine the appropriate action (such as return to CBTDEV proponent for further work, work the action at the MACOM headquarters, or some combination thereof). DCS, G–8 is also provided a draft copy for review and comment during this process. DCS, G–8 and other affected HQDA action officers should be familiar with the COIC since they are

members of the T&E WIPT. Opting to not be members of the T&E WIPT signifies that they have no input during the COIC approval process. See paragraph 4–5*c* for COIC staffing package guidance.

(3) Provide decision paper to the COIC approval authority. This includes at a minimum, the proposed COIC with approval memorandum or memorandum forwarding through CG, ATEC to DCS, G–8, DAPR–FDR, as applicable, the ORD–COIC crosswalk matrix, the MATDEV or PM and ATEC positions (concur or nonconcur), and a recommended course of action. Any nonconcurrence position by the MATDEV or PM or ATEC must either be resolved to the satisfaction of the key players (that is, CBTDEV, MACOM headquarters, MATDEV or PM, or ATEC) or if irresolvable, forwarded to DCS, G–8 for resolution. If there is an issue for resolution at HQDA, the forwarding memorandum will define the issue to be resolved and the differing positions from the principals.

(4) MACOM COIC forwarding through CG, ATEC to DCS, G–8 for approval. See paragraph 4–5*c* for submission memorandum guidance and paragraph F–5 for MACOM COIC approval memorandum guidance.

g. After the ORD is approved through the AROC (or the JROC for ACAT I programs), the MACOM headquarters submits the COIC through CG, ATEC to DCS, G–8 for approval. CG, ATEC confirms that the proposed COIC reflects agreement reached in final coordination (or properly defines any unresolved disagreement for DCS, G–8 resolution) and endorses the COIC to DCS, G–8 for action or approval. DCS, G–8 receives advance copy of the COIC from the CBTDEV/MACOM headquarters, schedules the necessary action (COIC approval or issue resolution) with the appropriate DCS, G–8 general officer, and initiates HQDA coordination. If there are no disagreements for resolution at the DCS, G–8 general officer level, the DCS, G–8 action officer uses the ORD–COIC crosswalk matrix and briefs the DCS, G–8 general officer to obtain COIC approval. If there are issues that need DCS, G–8 resolution before the COIC approval, the meeting with DCS, G–8 consists of the appropriate MACOM headquarters, MATDEV or PM, and ATEC representatives. CBTDEV proponent representative may also attend this meeting. Upon approval of the COIC, the DCS, G–8 general officer signs a memorandum forwarding the approved COIC to the PM or MATDEV for inclusion in the TEMP with copies furnished to the TEMA, CBTDEV MACOM headquarters action office; CG, ATEC; and the CBTDEV. See paragraph F–5 for DCS, G–8 COIC approval memorandum.

SAMPLE ORD-COIC CROSSWALK

Medical Communications for Combat Casualty Care (MC4) System

ORD Reference (*indicates a KPP)	Critical Operational Issues and Criteria
Supports the requirement that the Service supplied computer hardware used to run the TMIP software must meet the minimum hardware requirements stated in the TMIP TEMP. 1.f. (2) (a), page 10: The MC4 program will "develop the Army's infrastructure for the utilization of the Joint TMIP software." 4.a (2), page 28: The MC4 system has the mission to "provide the computer infrastructure for the Army's implementation of the Joint TMIP software. As needed, development software for Army-unique medical requirements not met by TMIP." *4.b (2) (a) i, page 31: The MC4 computer hardware must be able to run the operating system utilized by TMIP.	1.2.1.2 The MC4 computers must provide significant processor speed and memory capacity to run the TMIP software. 1.2.1.3 Any MC4 supplied software must be compatible with the TMIP software.

Figure F–2. Operational requirements document–critical operational issues and criteria crosswalk matrix

F–3. Critical operational issues and criteria process for non-tactical C4/IT programs

Figure F–3 depicts the COIC approval process for non-tactical C4/IT programs. The FP has lead responsibility while the CIO/G–6 approves all COIC.

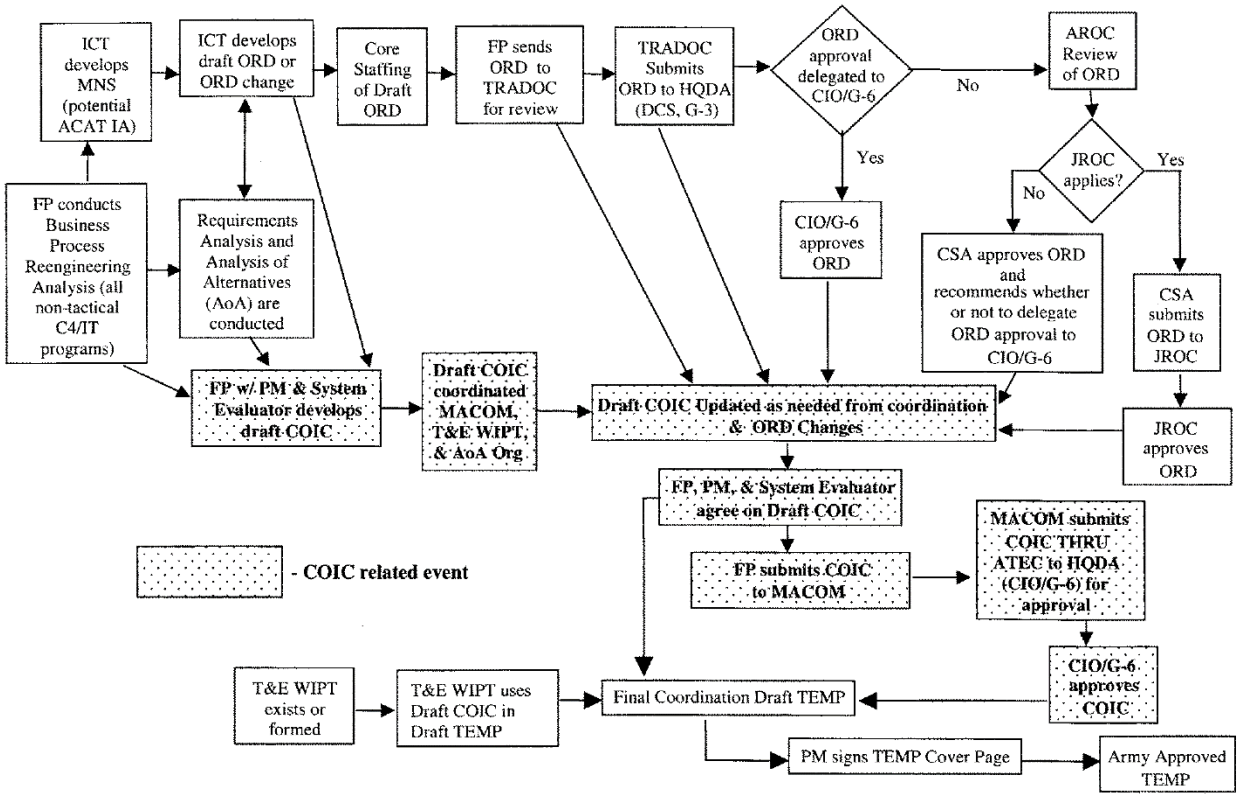


Figure F–3. Critical operational issues and criteria approval process for non-tactical C4/IT programs

a. The FP has lead for ORD and COIC development for non-tactical C4/IT programs. The FP initiates development of the ORD in response to an identified and approved information system need to support the Army infrastructure operations from a Business Process Reengineering analysis and, for ACAT IA programs, a JROC-approved MNS. The FP initiates COIC development by forming a team with the MATDEV or PM and system evaluator (normally from AEC) as an adjunct to the ICT developing and writing the ORD. COIC are based on ORD and the analyses supporting ORD development. Separate COIC and ORD development creates extra work for the FP, MATDEV or PM, and system evaluator either by revisiting analyses supporting ORD development to develop the COIC and/or by initiating changes to an approved ORD identified during COIC development. ORD and COIC development are complementary tasks and when properly executed much of the COIC content may be lifted directly from the ORD. ORD development will normally lead the COIC in the development processes. As the ORD enters core staffing, the team will finalize for coordination the initial draft COIC (or draft revision to the COIC in the case of a change or update to an approved ORD). Because of the COIC interrelationship with and dependence on the ORD, COIC will not be approved until the ORD is approved. Any change in an approved ORD KPP will normally require a change in the COIC. It was not always policy to extract KPP verbatim from the ORD for inclusion in COIC. Change in other approved ORD required capabilities or constraints may require a change in COIC. A change in previously approved COIC may require a change in the ORD.

b. As depicted in figure F–3, the draft COIC are readied for and begin coordination while the ORD is in core staffing. While the FP has lead for the product being coordinated, it is a team effort with the MATDEV or PM and system evaluator who have vested interest and must participate in the process and consider comments received. The MACOM provides comments and advice reflecting consideration of emerging MACOM operational concepts and strategic plans as well as cross MACOM experiences with requirements and COIC approval and application during acquisition. The T&E WIPT provides comments and advice concerning ability to answer (for example, methodologies available or needed, program resource implications, and risks of obtaining an erroneous answer) and proposes alternatives when applicable. The AoA organization provides comments and advice concerning accurate reflection of AoA findings in the COIC (that is, linkage between the AoA, ORD, and COIC) as well as the how models and simulations may be used in supporting the evaluation of COIC. The FP, MATDEV or PM, and system evaluator use these

comments along with the ORD changes from the Core Staffing to refine the draft COIC. Concerns that are irresolvable within the team are raised through command channels for resolution and, if necessary, to CIO/G–6 for adjudication. The refined draft COIC are provided to the T&E WIPT for use in the draft TEMP and to the MACOM headquarters for information and comment as appropriate. If this should result in further change to the draft COIC, the revised draft will be provided to T&E WIPT for inclusion in the draft TEMP and the MACOM headquarters.

c. COIC are based on the ORD; therefore, changes that occur to the ORD during its approval process must be reviewed for impact on the draft COIC. When an ORD change impacts the COIC, the needed refinement must be made to the draft COIC. The FP, MATDEV or PM, and system evaluator will participate and agree with the revisions. Copies of the revisions will be provided the T&E WIPT and MACOM headquarters.

d. The team agreement or identified areas of disagreement elevated to their leadership for resolution is key throughout the process. As the draft COIC are readied for entry into the approval process, these areas of agreement or disagreement are formalized for resolution in the approval process. Preference is that the ORD approval by CIO/G–6 occur before entry of COIC into the approval process, but it is recognized that this is not always possible considering demands of milestone decision points, TEMP approval schedules, and ORD approval processes. System COIC that require CIO/G–6 ORD approval (that is, ACAT III programs) will not proceed beyond the MACOM headquarters until the ORD is approved. The FP has the lead for the development of the COIC and is responsible for the operational relevance of the COIC and for the non-materiel DOTMLPF components supporting system's achievement of the COIC. The PM or MATDEV should nonconcur with the draft COIC if the current state of technology or planned program cannot deliver materiel (hardware and/or software) capable of satisfying the COIC by the FRP DR. Likewise, the system evaluator should nonconcur with the draft COIC if any of the COIC criteria and issues cannot be evaluated and answered for the FRP DR.

e. CIO/G–6 retains approval authority for COIC for all non-tactical C4/IT programs. MACOM headquarters must submit the COIC to CIO/G–6 (SAIS–ION). The Chief of Staff, U.S. Army (CSA) must have approved the ORD before the COIC are submitted to the CIO/G–6. ORD–COIC crosswalk matrix (see fig F–2) is included (both electronic and hard copy) in the submission package for use during the approval processing and brief. While paper copies are needed to document official submission, electronic copies serve to expedite approval processing. As a minimum, official concurrence must be provided by the MATDEV or PM and ATEC (may be by email or fax) with the proposed COIC before submission by the FP. A proponent unresolved nonconcurrence by either the MATDEV or PM or ATEC, will require resolution at the MACOM headquarters level or, in exceptional cases, the CIO/G–6 level before approval of the COIC. See paragraph 4–5*c* for COIC submission package guidance.

f. Upon receipt of COIC for approval processing from one of its FPs or within its headquarters, the MACOM headquarters COIC action agent will take the following actions:

(1) Determine status of ORD approval and confirm if ORD has been approved by CSA or JROC. ORD must be approved before MACOM headquarters forwards the COIC to CIO/G–6 for approval.

(2) Coordinate COIC with MATDEV or PM and ATEC for command position. There should be no surprises at the MACOM headquarters, MATDEV or PM, or ATEC when the COIC arrive since previous coordination by the CBTDEV, MATDEV, and system evaluator with the CBTDEV MACOM headquarters and its leadership is central to the COIC development process. Given this the case, the command positions should be received within 15 calendar days. If this is not the case and the proposed COIC represent a surprise to the MACOM headquarters, MATDEV or PM, or ATEC, the MACOM headquarters will determine the appropriate action: return to FP for further work, work the action at the MACOM headquarters, or some combination thereof. In any case, significantly longer processing times will result. CIO/G–6 is also provided a copy for review and comment during this process. The CIO/G–6 and other affected Army Staff action officers should be familiar with the COIC since they are members of the program T&E WIPT. Not being members of the T&E WIPT signifies they are not concerned or interested in a particular program and should have nothing to say. See paragraph 4–5*c* for COIC submission package guidance.

(3) Provide decision paper to the COIC approval authority including the proposed COIC with approval memorandum or memorandum forwarding through CG, ATEC to CIO/G–6, SAIS–ION, as applicable, the ORD–COIC crosswalk matrix, the MATDEV or PM and ATEC positions (concur or nonconcur), and a recommended course of action. Any nonconcurrence position by the MATDEV or PM or ATEC must either be resolved to the satisfaction of the three key players or if irresolvable at the FP MACOM headquarters level, forwarded to CIO/G–6 with the proposed COIC for resolution. If there is a disagreement for adjudication at HQDA, the forwarding memorandum will define the disagreement to be adjudicated and the differing positions from the principals (FP MACOM headquarters, MATDEV or PM, or ATEC).

(4) MACOM COIC approval authority sign the memorandum forwarding the COIC through ATEC to CIO/G–6 (SAIS–ION) for approval.

g. After the ORD is approved by HQDA through the AROC or the JROC processes, the MACOM headquarters submits the COIC through CG, ATEC to CIO/G–6 (SAIS–ION) for approval. CG, ATEC confirms that the proposed COIC reflects agreement reached in final coordination (or properly defines any unresolved issue for CIO/G–6 resolution) and endorses the COIC to CIO/G–6 for action/approval. CIO/G–6 (SAIS–ION) receives an advance copy of the COIC from the FP MACOM headquarters, schedules the necessary action (COIC approval or issue resolution) with the appropriate CIO/G–6 general officer and initiates Army Staff coordination. If there are no disagreements for adjudication at the CIO/G–6 general officer level, the CIO/G–6 action officer uses the ORD–COIC Crosswalk charts and briefs the CIO/G–6 general officer to obtain approval of the COIC. If there are disagreements that need CIO/G–6 adjudication before the COIC approval, the meeting with the CIO/G–6 general officer will be in two parts; the first is issue resolution, and the second is COIC approval. Appropriate FP MACOM headquarters, MATDEV or PM, and ATEC representatives will attend the meeting with CIO/G–6 general officer when resolution of an issue regarding the COIC applies. FP representative may also attend this meeting. Upon approval of the COIC, the CIO/G–6 general officer signs a memorandum forwarding the approved COIC to the PM or MATDEV for inclusion in the TEMP with copies furnished the TEMA, FP MACOM headquarters action office, CG, ATEC and the FP. See paragraph F–5 for the CIO/G–6 COIC approval memorandum.

Note. If the program is not on the OSD T&E Oversight List (see http://www.hqda.army.mil/tema) and does not have unresolved FP, MATDEV or PM, or ATEC disagreements, then a colonel (O–6) or civilian equivalent may approve the COIC for CIO/G–6.

F–4. Operational requirements document–critical operational issues and criteria–test and evaluation master plan schedule synchronization considerations

a. Table F–1 provides planning factors for preparing a synchronized schedule. Most have a range of days for completion by the activity. The CBTDEV or FP, MATDEV or PM, and system evaluator must determine what is right for the program. Some are outside their control and must be determined through coordination with other agencies or offices (for example, HQDA (DAMO–FMR/SAIS–ION) for matters regarding HQDA or JROC approval of the ORD).

b. Table F–2 identifies schedule dates that constitute alarms if not achieved. If these dates are missed, then ability to implement "work-around" solutions must be explored. If work-around solutions are not possible, an acquisition schedule slip is likely since conduct of a milestone depends on an approved TEMP being available. These dates are significant either for COIC approval or depend upon the actual COIC approval in order for the TEMP approval process to remain on schedule.

Table F–1
Planning factors for schedule synchronization

Event	Planning factor (calendar days)
ORD–COIC concurrent development	120–360
Core staffing of ORD	45–75
Proponent coordination of Draft COIC	30–45
Proponent submission of ORD to TRADOC	15–30
TRADOC validation of ORD	30–60
CIO/G–6 approval of non-tactical C4/IT ORD	30–60
AROC processing and CSA approval of ORD	105–165
JROC processing and approval of ORD (ACAT I or IA only)	120–180
Proponent, MATDEV, and system evaluator agree on COIC	30–60
Proponent forwards COIC to MACOM headquarters	1–30
PM and ATEC command position on COIC	15–30
MACOM headquarters review and forward COIC to HQDA	5–30
ATEC endorsement of COIC to HQDA	15
DCS, G–8 or CIO/G–6 approval of COIC	30–60
Include approved COIC into final TEMP	15–30

Table F–1
Planning factors for schedule synchronization—Continued

Final coordination of TEMP with T&E WIPT	45–60
T&E WIPT meet to resolve issues and sign TEMP	7–30
PM, PEO, ATEC, TRADOC/FP signs TEMP approval page	1–20
DUSA (OR) or other authority approves TEMP	15–30

Table F–2
Schedule critical events*

Event	Critical schedule for Headquarters, Department of the Army-approved critical operational issues and criteria	Critical schedule for major Army command-approved critical operational issues and criteria
Approved ORD	165	135
PM or MATDEV, system evaluator, and CBTDEV or FP agree on COIC	155	125
Proponent forwards COIC to MACOM	150	120
PM or MATDEV and ATEC COIC command position	130	100
MACOM forwards COIC through ATEC to HQDA	120	90
ATEC endorsement of COIC to HQDA	105	N/A
DCS, G–8 or CIO/G–6 approved COIC	90	N/A
Final TEMP to T&E WIPT for coordination	80	80
PM or MATDEV signs TEMP approval page	30	30
Army-approved TEMP	0	0

Notes:
* These schedule dates should not be used to set up a program schedule since to do so would be planning for failure, as there would be no margin for error. They should be used in the schedule as alarm dates indicating that the effort is off track and needs immediate attention.

F–5. Sample critical operational issues and criteria memoranda

Figures F–4 through F–11 are sample memoranda.

a. Figure F–4. Materiel or tactical C4I/IT–CBTDEV proponent COIC submission memorandum.
b. Figure F–5. Materiel or tactical C4I/IT–MACOM headquarters COIC position staffing memorandum.
c. Figure F–6. Materiel and tactical C4I/IT–MACOM headquarters COIC submission memorandum.
d. Figure F–7. Materiel and tactical C4I/IT–DCS, G–8 COIC approval memorandum.
e. Figure F–8. Non-tactical C4/IT–FP COIC submission memorandum.
f. Figure F–9. Non-tactical C4/IT–MACOM headquarters COIC position staffing memorandum.
g. Figure F–10. Non-tactical C4/IT–MACOM COIC submission memorandum.
h. Figure F–11. Non-tactical C4/IT–CIO/G–6 COIC approval memorandum.

MACOM CBTDEV Proponent Letterhead

Office Symbol (73-1) (date)

MEMORANDUM FOR MACOM HQ, ATTN: office symbol for COIC Action Office, appropriate address information

Subject: Critical Operational Issues and Criteria (COIC) for "X" System

1. References:

   a. AR 73-1 (7 Jan 02), subject: Test and Evaluation Policy.

   b. DA PAM 73-1 (30 May 03), subject: Test and Evaluation in Support of Systems Acquisition.

2. This memorandum forwards COIC for subject system (Encl 1) for HQDA approval per references a and b. These COIC will need to be forwarded to HQDA (DCS, G-8) for approval. The ORD-COIC Crosswalk Matrix is provided at enclosure 2 to support the approval process. These COIC were previously staffed with and concurred (or nonconcurred) in by PM and ATEC. (If there is an unresolved difference of position, describe it here.)

3. Point of contact is (name, office symbol, phone, and e-mail).

FOR THE COMMANDER:

2 Encl
as

XXXXXXXXXXXXXXXXXXX
Signature Block for
MACOM Proponent office

CF:
US ARMY TEST AND EVALUATION COMMAND, ATTN: (enter office symbol for the Evaluator Office), 4501 FORD AVENUE, ALEXANDRIA, VA 22302-1458
PM/MATDEV, ATTN: action office, appropriate address information

Figure F–4. Materiel or tactical C4I/IT—combat developer proponent critical operational issues and criteria submission memorandum

MACOM Letterhead

Office Symbol (73-1) S: (date)

MEMORANDUM FOR:
US ARMY TEST AND EVALUATION COMMAND, ATTN: CSTE-ZA (enter evaluators name), 4501 FORD AVENUE, ALEXANDRIA, VA 22302-1458
PROGRAM MANAGER/MATERIEL DEVELOPER for System X
MACOM HQ Staff Elements (as applicable)

Subject: Critical Operational Issues and Criteria (COIC) for "X" System

1. References:

a. AR 73-1 (7 Jan 02), subject: Test and Evaluation Policy.

b. DA PAM 73-1 (30 May 03), subject: Test and Evaluation in Support of Systems Acquisition.

2. This memorandum forwards final draft COIC for subject system for your concurrence in accordance with references a and b. This is the command position staffing of the COIC to recommend that the MACOM authority forward these COIC to HQDA (DCS, G-8) for approval. The CBTDEV proponent has previously coordinated these COIC with the PM/MATDEV and ATEC and received concurrence (or nonconcurrence). (If there is an unresolved difference of position, describe it here and request that ATEC and the PM address whether the disagreement continues.)

3. Request your position be provided this headquarters (ATTN: Office Symbol XX) not later than (two weeks). This will support TEMP approval by (date) as currently scheduled. Significant changes will be staffed with you before the COIC are submitted for approval. An expedited staffing technique will be used to maintain current approval schedule.

4. Point of contact is (name, office symbol, phone, and e-mail).

FOR THE MACOM DEPUTY CHIEF OF STAFF:

1 Encl

XXXXXXXXXXXXXXXXXXX
Signature Block for
MACOM STAFF OFFICE DIRECTOR

CF:
HQDA, ATTN: DAPR-FDR, WASHINGTON, DC, 20310-0700
MACOM Command/Center/School, ATTN: DCD and TSM for System X

Figure F–5. Materiel and tactical C4I/IT—major Army command headquarters critical operational issues and criteria position staffing memorandum

MACOM Letterhead

Office Symbol (73-1) (date)

MEMORANDUM THRU COMMANDER, U.S. ARMY TEST AND EVALUATION COMMAND, ATTN: CSTE-ZA, 4501 FORD AVENUE, ALEXANDRIA, VA 22302-1458

FOR DEPUTY CHIEF OF STAFF, G-8, ATTN: DIRECTOR, FORCE DEVELOPMENT, 700 ARMY PENTAGON, WASHINGTON, D.C. 20310-0700

Subject: Critical Operational Issues and Criteria (COIC) for "X" System

1. References:

a. AR 73-1 (7 Jan 02), subject: Test and Evaluation Policy.

b. DA PAM 73-1 (30 May 03), subject: Test and Evaluation in Support of Systems Acquisition.

2. This memorandum forwards the COIC for subject system (Encl 1) for DCS, G-8 approval per references a and b. An ORD-COIC Crosswalk Matrix is provided at enclosure 2 to support the approval process. These COIC were previously staffed with and concurred in by PM and ATEC (or nonconccurred in by one or both). (If there is an unresolved difference of position, describe it here.)

3. Point of contact is (name, office symbol, phone, and e-mail).

FOR THE COMMANDER:

2 Encl
as

XXXXXXXXXXXXXXXXXXX
Signature Block for
MACOM COIC Approval Authority

CF:
HQDA, ATTN: DAPR-FDR, WASHINGTON, DC 20310-0700 (Advance Copy)
US ARMY TEST AND EVALUATION COMMAND, ATTN: (enter office symbol for the Evaluator Office), 4501 FORD AVENUE, ALEXANDRIA, VA 22302-1458
PM for System X
MACOM Proponent Command/Center/School, ATTN: applicable DCD and TSM for System X

Figure F–6. Materiel and tactical C4I/IT—major Army command headquarters critical operational issues and criteria submission memorandum

DEPARTMENT OF THE ARMY
DEPUTY CHIEF OF STAFF, G-8
700 ARMY PENTAGON
WASHINGTON, DC 20310-0700

DAPR-FDR (73-1c) (date)

MEMORANDUM FOR PM/MATDEV address

SUBJECT: Critical Operational Issues and Criteria (COIC) for "X" System

1. Reference, memorandum, MACOM, office symbol, date, subject as above.

2. COIC proposed by referenced memorandum are approved without change (or with the following changes).

3. The COIC at enclosure 1 include those changes addressed above and are being forwarded for inclusion in the system TEMP.

4. Point of contact for this action is (name, office symbol, phone, and e-mail).

1 Encl
as

XXXXXXXXXXXXXX
Signature Block for
Director, Force Development

CF:
TEST AND EVALUATION MANAGEMENT AGENCY, ATTN: DACS-TE, ROOM 2C139A, 200 ARMY PENTAGON, WASHINGTON, D.C. 20310-0200
US ARMY TEST AND EVALUATION COMMAND, ATTN: (enter office symbol for the Evaluator Office), 4501 FORD AVENUE, ALEXANDRIA, VA 22302-1458
MACOM HQ COIC Action Office
MACOM CBTDEV Proponent Command/Center/School, DCD or TSM for System X

Figure F–7. Materiel and tactical C4I/IT—Headquarters, Department of the Army (Deputy Chief of Staff, G–8) critical operational issues and criteria approval memorandum

MACOM Functional Proponent Letterhead

Office Symbol (73-1) (date)

MEMORANDUM FOR MACOM HQ, ATTN: office symbol for COIC Action Office, appropriate address information

Subject: Critical Operational Issues and Criteria (COIC) for "X" System

1. References:

a. AR 73-1 (7 Jan 02), subject: Test and Evaluation Policy.

b. DA PAM 73-1 (30 May 03), subject: Test and Evaluation in Support of Systems Acquisition.

c. HQDA, TEMA Web Site (http://www.hqda.army.mil/tema/temp_status.doc), OSD and HQDA T&E Oversight List.

2. This memorandum forwards COIC for subject system (Encl 1) for MACOM HQ approval and forwarding to CIO/G-6 (SAIS-ION) for approval per references a and b. These COIC are for a program that is (is not) on the OSD T&E Oversight List (reference c). The ORD-COIC Crosswalk Matrix is provided at enclosure 2 to support the approval process. These COIC were previously staffed and concurred with by PM and ATEC (or nonconcurred in by one or both). (If there is an unresolved difference of position, describe it here.)

3. Point of contact is (name, office symbol, phone, and e-mail).

FOR THE COMMANDER:

2 Encl
as

XXXXXXXXXXXX
Signature Block for
MACOM Proponent office

CF:
US ARMY TEST AND EVALUATION COMMAND, ATTN: (enter office symbol for the Evaluator Office), 4501 FORD AVENUE, ALEXANDRIA, VA 22302-1458
PM/MATDEV, ATTN: action office, appropriate address information for System X

Figure F–8. Non-tactical C4/IT—functional proponent critical operational issues and criteria submission memorandum

MACOM Letterhead

SAIS-ION (73-1) S: (date)

MEMORANDUM FOR:
US ARMY TEST AND EVALUATION COMMAND, ATTN: CSTE-ZA (enter evaluator's name), 4501 FORD AVENUE, ALEXANDRIA, VA 22302-1458
PROGRAM MANAGER/MATERIEL DEVELOPER for System X
MACOM HQ Staff Elements (as applicable)

Subject: Critical Operational Issues and Criteria (COIC) for "X" System

1. References:

a. AR 73-1 (7 Jan 02), subject: Test and Evaluation Policy.
b. DA PAM 73-1 (30 May 03), subject: Test and Evaluation in Support of Systems Acquisition.
c. HQDA, TEMA Web Site (http://www.hqda.army.mil/tema/temp_status.doc), OSD T&E Oversight List.

2. This memorandum forwards final draft COIC for subject system for your concurrence in accordance with references a and b. These COIC are for a program that is (is not) on the OSD T&E Oversight List (reference c). This is the command position staffing of the COIC to recommend that the MACOM authority forward these COIC to HQDA for CIO/G-6 approval. The functional proponent has previously coordinated these COIC with the PM/MATDEV and ATEC and received concurrence (or nonconcurrence). (If there is an unresolved difference of position, describe it here and request that ATEC and the PM address whether the disagreement continues.)

3. Request your position be provided this headquarters (ATTN: Office Symbol XX) not later than (two weeks). This will support TEMP approval by (date) as currently scheduled. Significant changes will be staffed with you before the MACOM authority forwards the COIC for HQDA approval. Expedited staffing will be used to maintain current approval schedule.

4. Point of contact is (name, office symbol, phone, and e-mail).

FOR THE MACOM DEPUTY CHIEF OF STAFF:

1 Encl

XXXXXXXXXXXX
Signature Block for
MACOM STAFF OFFICE DIRECTOR

CF:
HQDA, ATTN: SAIS-ION, 107 ARMY PENTAGON, WASHINGTON, DC 20310
MACOM Functional Proponent for System X

Figure F–9. Non-tactical C4/IT—major Army command headquarters critical operational issues and criteria position staffing memorandum

MACOM Letterhead

Office Symbol (73-1) (date)

MEMORANDUM THRU COMMANDER, U.S. ARMY TEST AND EVALUATION COMMAND, ATTN: CSTE-ZA, 4501 FORD AVENUE, ALEXANDRIA, VA 22302-1458

FOR: HQDA, ATTN: SAIS-ION, 107 ARMY PENTAGON, WASHINGTON, D.C. 20310

Subject: Critical Operational Issues and Criteria (COIC) for "X" System

1. References:

a. AR 73-1 (7 Jan 02), subject: Test and Evaluation Policy.

b. DA PAM 73-1 (30 May 03), subject: Test and Evaluation in Support of Systems Acquisition.

c. HQDA, TEMA Web Site (http://www.hqda.army.mil/tema/temp_status.doc), OSD T&E Oversight List.

2. This memorandum forwards the COIC for subject system (Encl 1) for the HQDA (CIO/G-6) approval per references a and b. These COIC are for a program that is (is not) on the OSD or HQDA T&E Oversight List (reference c) and therefore will (or will not) require general officer or civilian equivalent level approval. An ORD-COIC Crosswalk Matrix is provided at enclosure 2 to support the approval process. These COIC were previously staffed and concurred with by PM and ATEC (or nonconcurred in by one or both). (If there is an unresolved difference of position, describe it here.)

3. Point of contact is (name, office symbol, phone, and e-mail).

FOR THE COMMANDER:

2 Encl
as

XXXXXXXXXXXX
Signature Block for
MACOM STAFF OFFICE DIRECTOR

CF:
US ARMY TEST AND EVALUATION COMMAND, ATTN: (enter office symbol for the Evaluator Office), 4501 FORD AVENUE, ALEXANDRIA, VA 22302-1458
PM for System X
MACOM Functional Proponent for System X

Figure F–10. Non-tactical C4/IT—major Army command critical operational issues and criteria submission memorandum

HQDA (CIO/G-6) Letterhead

SAIS-ION (73-1c) (date)

MEMORANDUM FOR PM/MATDEV address

SUBJECT: Critical Operational Issues and Criteria (COIC) for "X" System

1. Reference, memorandum, MACOM, office symbol, date, subject as above.

2. COIC proposed by referenced memorandum are approved without change (or with the following changes).

3. COIC at enclosure 1 include those changes addressed above and are ready for inclusion in the system TEMP.

4. Point of contact is (name, office symbol, phone, and e-mail).

1 Encl
as

XXXXXXXXXXXX
Signature Block for
General Officer, COIC Approval Authority

CF:
TEST AND EVALUATION MANAGEMENT AGENCY, ATTN: DACS-TE, ROOM 2C139A, 200 ARMY PENTAGON, WASHINGTON, D.C. 20310-0200
US ARMY TEST AND EVALUATION COMMAND, ATTN: (enter office symbol for the Evaluator Office), 4501 FORD AVENUE, ALEXANDRIA, VA 22302-1458
MACOM HQ COIC Action Office for System X
MACOM Functional Proponent for System X

Figure F–11. Non-tactical C4/IT—Headquarters, Department of the Army (CIO/G–6) critical operational issues and criteria approval memorandum

Appendix G

Critical Operational Issues and Criteria Checklist

G–1. Use of the critical operational issues and criteria checklist

a. The COIC Checklist should be used by COIC preparers, staffers at all levels, and by those individuals involved in the preparation, review, and approval of COIC. The COIC checklist covers—

(1) Format and content.

(2) HQDA review and approval.

b. The COIC checklist applies to materiel, tactical C4I/IT, and non-tactical C4/IT systems. All questions are intended to be answered "yes." If a question is answered "no," the applicable element should be reworked or justification provided.

G–2. Critical operational issues and criteria format and content

a. Heading.

(1) Does it state, "Critical operational issues and criteria for"?

(2) Does it contain the system name?

(3) Does it identify the applicable TEMP?

b. Format.

(1) Is there a scope, criteria, and rationale paragraph for each issue?

(2) Does paragraph numbering follow the dendritic format of X.0–Issue, X.1–Scope, X.2–Criteria, and X.3–Rationale? (X is the issue number; for example, 1 or 2.)

(3) Does each criterion have an associated rationale subparagraph?

(4) Are the mandatory notes and other system peculiar notes included?

c. Content—Issues.

(1) Do the issues reflect only those few key operational concerns for determining the system's readiness at the FRP DR?

(2) Are the issues in the form of questions to be answered "yes" or "no" (that is, no issue should be investigative in nature—"How well" or "What is")?

(3) Are the issues based on the MNS?

(4) Are the issues operationally realistic and do they ask if/whether a task/function or mission can be achieved?

(5) Do the issues focus on the total operational system and not its component parts?

(6) Do the issues focus the decision? (They should not over generalize, for example, "Is system X operationally effective/sustainable in an operational environment?")

(7) Are issue statements free of criteria (for example, performance standards)?

(8) Has overlapping coverage between issues been avoided to the degree possible and appropriate?

d. Content—Scope.

(1) Does the scope identify the operational capabilities to be examined?

(2) Are terms peculiar to the system and evaluation of each issue defined?

(3) Are the tactical context and scenarios applicable to the evaluation of each issue identified?

(4) Are key system deployment and organizational structure factors applicable to the evaluation identified?

(5) Are applicable approved threat documents referenced?

(6) Are applicable crew and maintainers identified?

(7) Are key natural and battlefield environments identified?

(8) Have requirements for technical testing and modeling analysis been identified?

(9) Is the scope free of criteria and requirements statements?

(10) Is the scope free of requirements for statistical confidence levels applicable to the criteria?

e. Content—Criteria.

(1) Is there at least one criterion for each critical operational issue?

(2) Is each criterion a showstopper for the FRP decision? Would you say no to FRP if the criterion was not satisfied based on what you know now?

(3) Do the criteria represent a performance threshold (for example, quicker delivery of mission/operational orders (MS B TEMP) or delivery of mission/operational orders within 1 hour on the average after initiation of operations (MS C TEMP))?

(4) Are the criteria few in number (on the average about 10 is right significantly fewer for single shot item and more for a family-of-systems) about 2 to 4 per issue normally?

(5) Has the PM or MATDEV confirmed that the criteria are technically feasible and achievable by FRP DR within the planned program?

(6) Does the system evaluator have a viable concept for evaluating the criteria and can this plan be executed within the program?

(7) Can the necessary doctrine, TTP, training, leader developments, organization, and Soldier products be developed, matured and ready for the player unit for IOT to support achievement of these criteria?

(8) Are all criteria based on or derived from requirements documented in the ORD and AoA and do they reflect the critical operational needs and constraints? (The criteria do not have to be a direct lift but must be traceable to approved ORD and AoA.)

(9) Do the criteria reflect a level of system maturity appropriate to the milestone TEMP (for example, "soft" for MS B but "firm" for MS C)?

(10) Has overlapping coverage among criteria been avoided to preclude multiple failure for a single shortfall?

(11) Are all criteria that are not total operational system measures (the preference) fully justifiable (operational FRP decision showstoppers)?

(12) Do criteria reflect only essential operational requirements (not desired capabilities)?

(13) Wherever possible, are higher order MOPs (for example, probability of kill, or probability of successful communications) stated rather than those of contributing components (for example, individual probabilities for detecting, engaging, hitting, and killing a target; and probabilities for connectivity message accuracy and RAM)?

(14) Do the criteria avoid the use of force exchange ratio, loss exchange ratio, or similar operational effectiveness measures more appropriate for AoA/modeling? If used, have M&S analyses been required in the scope paragraph to expand beyond trials available in test?

(15) Is a baseline comparison used only when a specific performance measure cannot be derived, when directed by higher authority, or to reduce the chance of bias during T&E?

(16) If a baseline comparison is used, and performance improvement is the objective, is an improvement percentage specified?

(17) Are qualitative criteria measurable?

(18) Are all constraint conditions applicable to evaluation of each criteria stated and consistent with the scope (for example, MOPP IV and EW)? They may also be included in the system peculiar notes.

(19) Are all definitions applicable to evaluation of each criterion stated and consistent with the scope (for example, firepower kill, and payload)? They may also be included in the system peculiar notes.

(20) Have potential ambiguities which could result in erroneous T&E been avoided?

(21) Are probabilistic criteria used when man-machine interface dependent (for example, X percent of attempts or median time)?

(22) Is the appropriate level system (that is, individual system, team, and platoon) addressed by each criteria? (Criteria must be the lowest level appropriate for the system—an individual system is preferred; an organizational element should be used when the system's primary mission contributes to unit performance.)

(23) Are all MOPs critical to the FRP decision covered? (No key criteria should be excluded because the data source was other than operational test or problems collecting needed data were anticipated.)

(24) Are criteria free of confidence levels?

f. Content—Rationale.

(1) Do the rationale statements justify each criterion?

(2) Are reasons stated for selecting the characteristic/capability used?

(3) Are the ORD and other source document paragraph references identified?

(4) Are complete references provided for criteria derived by combining characteristics or capabilities?

(5) Is an audit trail to the AoA provided?

g. Content—Notes.

(1) Are mandatory notes #1 and #2 present?

(2) Have total operational system criteria been identified in mandatory note #1?

(3) Is mandatory note #3 present for COIC in support of the MS B TEMP?

(4) Are notes peculiar to the system, as referenced in the body of the COIC, provided?

G–3. Critical operational issues and criteria review and approval—systems requiring approval by Headquarters, Department of the Army (Deputy Chief of Staff, G–8 and CIO/G–6)

a. For MACOM, headquarters forwarding to HQDA—

(1) Is the ORD approved?

(2) Are the following coordinations complete:

(a) Proponent—coordination with PM or MATDEV and ATEC?

(b) Headquarters, MACOM—command position coordination within headquarters MACOM and with PM or MATDEV, ATEC and the action officer in DAPR–FDR or SAIS–ION?

(3) Have all concurred with the COIC? (If "No," strong rationale must be provided for MACOM, headquarters COIC approval authority consideration.)

(4) Are the ORD–COIC Crosswalk Matrices ready?

b. For DCS, G–8 and CIO/G–6 approval—

(1) Does the COIC MACOM headquarters forwarding memo contain the ORD–COIC crosswalk matrix?

(2) Has the CG, ATEC and the PM or MATDEV concurred with the COIC?

(3) If the CG, ATEC or the PM or MATDEV nonconcurred and MACOM headquarters disagrees with the nonconcurrence, has a joint CG, ATEC; PM or MATDEV; MACOM headquarters; and DCS, G–8 or CIO/G–6 COIC approval authority forum been set for resolution?

(4) Have the appropriate DA staff elements concurred with the COIC?

Appendix H

Critical Operational Issues and Criteria Development Example

H–1. Example

This appendix provides a situation and a school solution regarding a COIC development example. It is intended to demonstrate the thought process involved in developing a set of COIC with few issues and criteria defining a good enough system for FRP. This is a fictitious case based on actual cases.

H–2. Situation and solution

See figures H–1 and H–2 for the example and solution.

***The Situation*:**

System -- Communications system including radio set (component of the user system) and net control station (NCS) with generator, vehicle, and crew.

Need -- High speed, secure and nonsecure, jam resistant data communications for automated systems.

Mission -- Deploy to theater of operations, set up, initialize net, provide continuous communications support, and relocate components (frequently) to survive.

Deployment -- Light forces divisions through battalion command posts and key operational units.

Employment
- Combined and joint operations control
- Division systems control manages net
- NCS support (dedicated team with vehicle)
- Radio set support (standard logistics)

Acquisition Strategy
- Developmental system (NCS and radio set)
- Uses standard truck, shelter, and generator
- ORD and MS B completed
- ORD being updated for MS C (LRIP based on technical and early user tests)
- FRP Decision (full-rate production based on developmental tests and IOT)

ORD Requirements Emphasis
- Connectivity between users (communications link exists)
- Continuity of operations during movement and maintenance
- NCS set up, tear down, and net initialization times
- Aerial deployment for NCS (radio certified with user)
- Allied and combined operations interoperability
- RAM for NCS and radio set

ORD Requirements
1. User connectivity 90% of the time in a benign environment.
2. User connectivity 80% of the time in an electronic warfare (EW) environment.
3. User through-put (messages/hour) identified by the user.
4. User speed of service requirement identified by the user (not more than a factor of 3 degradation in an EW environment for priority messages).
5. Continuity of net operations (NCS/radios) during movement and maintenance.
6. NCS roll-on/off transportability via C-130.
7. NCS certified for air drop and deployment.
8. NCS set up (first radio in net) within 45 minutes.
9. NCS tear down and depart site within 45 minutes.
10. High-altitude electro-magnetic pulse (HAEMP) and nuclear, biological, and chemical contamination (NBCC) survivable.
11. Employed in hot, basic, and cold climates.
12. Communications interface with allied and other service communications systems used with automated control systems.
13. School NCS training will include training device (one trainer station and four (4) student stations); unit sustainment training will be supported by an exportable training package.
14. Reliability, availability, and maintainability (RAM): NCS A_o .9, Mean Time Between Operational Mission Failure (MTBOMF) 300 HR, and Maintenance Ratio (MR) 0.002; Radio Set A_o .95, MTBOMF 300 HR, and MR 0.0005

Specification Requirement -- 90% throughput success and 90% speed of service success given user connectivity exists.

Figure H–1. The situation

Operational Mode Summary/Mission Profile (OMS/MP) -- NCS set up within 45 minutes, operate for 2 hours, tear down within 45 minutes, movement 1 hour, 24 hour/day operations; radio set IAW user system OMS/MP.

Approved COI for Another Communications System

- Three Issues -- Does/Can it:
  - ----- Provide secure voice and data communications which meets the user's need.
  - ----- Deploy from garrison to field and operate IAW OMS/MP.
  - ----- System with logistics sustain combat operations.
- Key criteria:
  - ----- Probability of a message being sent and received in benign and EW environments.
  - ----- Movement to field site in a single lift.
  - ----- Set up and tear down times.
  - ----- Sustained combat operations for 30 days.

Other Considerations

- Development test to verify technical characteristics.
- DIA approved threat package and scenario to be used in the initial operational test (IOT).
- IOT to test total operational system.
- Doctrine and Organization Test Support Package (TSP) to be used for employment in the IOT.
- COIC guidance: Sustainment COIC for a control system should address training maintaining proficiency in the unit and logistics sustaining combat operations for a period of time.
- Approved COIC for another system included.

Figure H–1. The situation—Continued

A Solution:

Critical Operational Issues and Criteria (COIC)
for the AN/GRC-986(V) Communications System
for Test and Evaluation Master Plan (TEMP) Supporting
Milestone C

1.0 ***Issue:*** Does the AN/GRC-986(V) system provide high speed, secure and non-secure, jam resistant data communications for light forces automated control systems?

1.1 ***Scope:*** This issue examines the capability of the AN/GRC-986(V) to provide high speed, secure and non-secure, jam resistant communications support for light forces, to include combined and joint operations. A division slice will be played with radios for allies and other services control systems in a net. Communications measure of performance to be examined will be percentage of message traffic passed. The AN/GRC-986(V) will be operated and maintained by qualified soldiers in accordance with the Operational Mode Summary/Mission Profile (OMS/MP). Continuity of operations during movement and maintenance will occur as a normal part of operations. Employment will be in accordance with the Doctrinal and Organizational Test Support Package (TSP). MOPP IV level operations will be simulated.

1.2 ***Criterion:*** The AN/GRC-986(V) will pass at least 73% of the user required priority message traffic to the correct addressee within the user specified speed of service (SOS) (see note 3) in a benign environment, and at least 65% of priority messages with no more than a factor of 3 degradation in SOS in a threat EW environment.

1.3 ***Rationale:*** The AN/GRC-986(V) mission effectiveness is its capability to deliver information to the correct addressee in time to take necessary action. Criterion 1.2 was derived from ORD requirements paragraphs 1, 2, 3, and 4 (connectivity in benign and EW environments, throughput, and SOS) and specification requirements for 90% throughput and 90% SOS. Benign percentage = .9 X .9 X .9 X 100 = 73%. EW percentage = .8 X .9 X .9 X 100 = .65.

2.0 ***Issue:*** Does the AN/GRC-986(V) system provide joint, combined, and intra-Army interoperability required to support light force operations.

2.1 ***Scope:*** This issue examines the ability of the AN/GRC-986(V) to interface with key joint, combined, and intra Army systems and exchange information as needed by light forces. Operations will be IAW the OMS/MP and the Doctrine and Organizational TSP. Threat representation will be IAW the Threat TSP.

2.2 ***Criterion:*** The AN/GRC-986(V) will interface with allied, other service, and intra-Army systems identified in note 4 and exchange information IAW with parameters set forth in the information exchange requirements matrix at note 4.

2.3 ***Rationale:*** For the AN/GRC-986(V) to effectively support light forces communications, it must at least interface with those systems identified at note 4 accomplish the exchanges specified. This criterion is an ORD KPP and is paragraph 4b(1) of the ORD. As per the KPP paragraph only those information exchange requirements identified as critical are included in note 4. The AoA supports the need for these interfaces.

3.0 ***Issue:*** Can the AN/GRC-986(V) be deployed from garrison to a field site while operating in accordance with the OMS/MP?

3.1 ***Scope:*** This issue examines the deployability of the AN/GRC-986(V) as a total operational system, that is, shelter/truck, mounted radio set, and NCS with organic generator. Specific modes/techniques of deployability addressed will be roll-on/roll-off and aerial delivery via Low Velocity Air Drop (LVAD) from C-130 aircraft. The crew will be deployed by separate aircraft. Additionally, data will be collected in benign and NBC (MOPP IV) environments in the time required to prepare the system (set up) for operation following crew/equipment link-up and/or arrival at the operations site, and to prepare the system (tear down) for survivability moves.

Figure H–2. A solution

3.2 *Criteria*:

3.2.1 The AN/GRC-986(V) net control station must be certified for the following transport and deployment methods:

a. Roll-on and roll-off transport by C-130.
b. LVAD (air drop) delivery.

3.2.2 The NCS crew must set up and have the first radio in the net within 45 minutes 90% of the time (time starts upon arrival on site). When dressed in MOPP IV, 60 minutes is allowed.

3.2.3 The NCS crew will tear down and depart site with median time less than 45 minutes after receipt of the move order. A median time of 60 minutes is allowed when dressed in MOPP IV

3.3 *Rationale*: While the AN/GRC-986(V) NCS will be transported via all modes, aerial deployability is most critical to light units. The NCS must be like deployable to the users it supports. The NCS must move to survive during combat.

3.3.1 Criterion 3.2.1 is derived from ORD paragraphs 6 and 7.

3.3.2 Criterion 3.2.2 comes from ORD requirement paragraph 8. Applying a 90 percent factor recognizes the possibility of shortfalls under realistic operational conditions. Set up is considered more time sensitive than tear down. An allowance of 15 additional minutes is made for MOPP IV degradation.

3.3.3 Criterion 3.2.3 is based on ORD requirement paragraph 9, with similar considerations to those for criteria 3.2.2. Median time is considered realistic for tear down.

4.0 *Issue*: Can AN/GRC-986(V) equipped units achieve training proficiency in garrison and provide a wartime readiness capability for sustained combat operations?

4.1 *Scope*:

4.1.1 This issue examines sustainment training provided to NCS crews. The unit training device, training publications and literature, and methods of instruction included in the program of instruction will be addressed. Training adequacy will be examined in terms of operator proficiency in performing critical tasks required to effectively employ the AN/GRC-986(V) (the critical tasks and standards to be met will be identified in the New Equipment Training TSP). Questionnaires and structured interviews with the test participants, instructors, and test directorate personnel regarding the adequacy of training, the training device, training materials, and operator acceptability of training manuals in accordance with AR 25-30 will be conducted. Also addressed will be correctness, applicability, format, degree of detail, and ease of use of publications.

4.1.2 This issue also encompasses an evaluation of the maintenance concept, the system support package (SSP), and PLL/ASL under realistic operational conditions. To be examined are the dedicated NCS maintenance team, and logistics support hardware and software needed to support the system. Hardware includes tools and test equipment. Software includes technical manuals, repair parts and special tools listings, the maintenance allocation chart (MAC), and parts allocation tables. Operational conditions will include movement to enhance survivability.

4.2 *Criteria*:

4.2.1 The AN/GRC-986(V) NCS crews will be able to practice and perform crew drills in garrison. 95% of the representative soldier operators must be capable of performing all critical tasks for their respective MOS to the assigned training standard.

4.2.2 The dedicated NCS maintenance teams (one per NCS), with allotted tools, test equipment, and repair parts, will sustain a division operation for a period of 30 days without negative impact on continuity of operations.

Figure H–2. A solution—Continued

4.3 ***Rationale*****:** Units will come to combat "as is;" therefore, they must maintain proficiency during peacetime and be capable of sustaining operations until the logistics system catches up.

4.3.1 Criterion 4.2.1 is based on ORD requirement paragraph 13, which plans for an exportable packet for sustainment training.

4.3.2 Criterion 4.2.2 is based on ORD requirement paragraph 14 and the support concept of providing a dedicated maintenance teams for the NCS. The 30-day sustainment factor is minimum essential to allow the logistics system to catch up.

Note 1: Criteria are for total operational system measures. As such, they inherently cover hardware, software, personnel, doctrine, organization, and training. System individual characteristics of operational capability, survivability, RAM, organization, doctrine, tactics, logistics support, training, and MANPRINT (which includes the domains of manpower, personnel, training, human factors engineering, system safety, health hazards, and soldier survivability) related to these criteria will be provided by the system evaluator in the system evaluation plan.

Note 2: Criteria are not provided as automatic (default) pass/fail measures. Rather, they represent estimates of performance for which a breach would require a careful senior level management reassessment of cost effectiveness and program options during the program milestone decision review.

Note 3: This note would contain a definition of user specified speed of service (SOS).

Note 4: This note would contain a listing of Allied and other Service systems with which the AN/GRC-986(V) is required to be interoperable for data exchange and information exchange requirement (IER) matrix. The matrix would only present the critical IERs from the ORD applicable to this FRP decision.

Figure H–2. A solution—Continued

Appendix I

Survivability and Vulnerability Issue: System Evaluation Considerations

I–1. Overview of the survivability evaluation process

The survivability T&E process is part of the CE process. As part of that process, the evaluation must address design or configuration changes that could affect the system's survivability. Survivability requirements can change as a result of emerging technology, evolving threats, and increasing dependence on global information systems.

a. The survivability of Army weapon systems, automated information systems (AISs), and other materiel directly impacts system effectiveness and suitability, and consequently, mission accomplishment. The survivability approach must address the system's capabilities to avoid/evade (for example, through non-materiel solutions such as TTPs) as well as withstand the effects of expected threats. The survivability evaluation addresses the following areas that are discussed in more detail in paragraph I–5:

(1) Electromagnetic environmental effects (E3).
(2) Information assurance (IA).
(3) Nuclear, biological, and chemical (NBC).
(4) Nuclear weapon effects (NWE).
(5) Electronic warfare (EW).
(6) Obscurants and atmospherics.
(7) Soldier survivability.
(8) Ballistic effects.

b. Each survivability evaluation is focused on the susceptibilities of the system and tailored to address the operational requirements of the CBTDEV. The methodology incorporates the CBTDEV's mission critical tasks for the candidate system and addresses operational implications of survivability, including the Soldier and TTPs, in the survivability measures.

I–2. Definition and requirements

a. Survivability is defined in the Defense Acquisition Guidebook as "the capability of a system and crew to avoid or withstand a manmade hostile environment without suffering an abortive impairment of its ability to accomplish its designated mission." The Defense Acquisition Guidebook stipulates, "Unless waived by the MDA, mission critical systems, regardless of ACAT, will be survivable to the threat levels anticipated in their operating environment. System (to include the crew) survivability from all threats found in the various levels of conflict will be considered and fully assessed as early as possible in the program, usually during System Development and Demonstration." Survivability against the full spectrum of battlefield threats must be considered in all system acquisition programs, including new developments, NDI acquisition, and system modifications/upgrades that can impact the system's ability to withstand the specified threats.

b. Survivability requirements are incorporated in the planning and execution of all aspects of a system's acquisition life cycle. CBTDEVs coordinate the formulation and staffing of survivability requirements during the drafting of the MNS and the ORD. The threat statements and operational environments specified in the MNS guide the preliminary survivability planning. The ORD identifies the survivability thresholds and objectives, defines Soldier and system survivability requirements, and identifies the expected threats to the system. The STAR delineates the current and projected threats that should be incorporated into the system's survivability requirements.

I–3. Survivability analyst responsibilities

The survivability analyst has the following unique responsibilities as a member of the system T&E team—

a. Ensure consistency among the STAR, ORD, SEP, and TEMP regarding expected survivability threats and requirements and the tests and analyses that must be conducted to provide input to the evaluation.

b. Define the survivability T&E issues.

c. Coordinate and clarify the survivability evaluation requirements with the combat and MATDEVs and the threat community.

d. Develop the IA survivability risk assessment.

e. Develop the survivability input to the TEMP, evaluation plans, and reports.

f. Guide and support survivability analysis, test planning, and data collection as well as related T&E efforts.

g. Conduct and report the survivability evaluation.

I–4. Survivability test and evaluation process

The following details the specific steps and procedures necessary to ensure an efficient and effective survivability T&E process. Most of these steps are unique to the survivability evaluation and should be considered in addition to the basic steps for any evaluation.

a. Review and establish the survivability requirements. System documentation that provides information about the survivability requirements of a system includes the ORD, STAR, and the system description. In addition, the COIC, OMS/MP, and discussions with the CBTDEV are necessary in formulating a survivability evaluation approach that is reasonable, credible, and tailored for the Army's intended use of the system consistent with the critical tasks identified by the user. As appropriate, the analyst should identify AI and measures in developing the survivability portion of the evaluation plan to cover those issues not addressed by the ORD and COIC. HQDA and DoD guidance and policies provide the regulatory basis for formulation of survivability requirements.

b. Gather a complete system description and determine system susceptibilities to the specified threats. System descriptions, configurations, and operational profiles are necessary to determine the significance of the expected battlefield threats. Key system information required as input for survivability evaluation planning includes the following:

(1) Descriptions of the system structure and component parts to determine their primary physical attributes such as electronic, mechanical, digital, RF, optical, electro-optical, and explosive.

(2) Functions of the system and its components.

(3) System deployment/employment (for example, intended interfaces with other systems, protection afforded by enclosures, mounted on a vehicle or dismounted, used in the rear echelon or front line, used in special operations, and used in a stationary or moving mode).

(4) Impact of a component failure on the functioning of the system (for example, Is system survivability lost or degraded? Does the loss of function of some components in the system degrade system survivability? Are such degradations acceptable?).

(5) Threats to the system and its components. Each component in a system will have certain levels of susceptibility to various threats. Components may be susceptible to the same threats or may be uniquely susceptible to a specific threat. Intra-system (as well as inter-system) components can be a threat to each other due to mutual incompatibilities. The overall susceptibility of the system to the threat environment is an aggregate of the susceptibilities of the system components.

(6) Mission impact (that is, So what? How does the degradation affect the system's ability to complete its mission? How does the degradation affect completion of the unit's mission?).

I–5. Survivability evaluation considerations

The following considerations are addressed in the survivability evaluation. The specific models identified in this paragraph are listed as examples only.

a. E3 evaluation:

(1) E3 refer to the impact of the electromagnetic environment on the operational capability of military forces, equipment, systems, and platforms. E3 threats can come from both hostile and friendly sources and may be either internal or external to the system. Due to the growing complexity of the command and control elements of weapon systems, increased verification of full up system compatibility to E3 environments is required. The Defense Acquisition Guidebook provides guidance for E3 and Spectrum Supportability. Additionally, DOT&E's Policy on Operational Test and Evaluation of Electromagnetic Environmental Effects and Spectrum Management more clearly defines the role of OT&E in identifying potentially adverse E3 situations. Two MIL–STDs that provide specific system level requirements for E3 are MIL–STD–461 and MIL–STD–464.

(2) The predominant Government E3 test facilities are located at ATC, MD; U.S. Army Redstone Technical Test Center (RTTC), AL; EPG, AZ; and WSMR, NM. Test facilities are also located at Patuxent River Naval Air Warfare Center and various Government contractor facilities. Data for the E3 evaluation may also come from sources such as the E3 database maintained by the Joint Spectrum Center, Annapolis, MD, and models such as the Unified E3 (UE3) and General Electromagnetic Model for the Analysis of Complex Systems (GEMACS). GEMACS and its related software enable an electromagnetic analyst to study various electromagnetic phenomena associated with antennas, radiation, emissions, coupling, electromagnetic interference (EMI)/EMC, and electromagnetic pulse (EMP).

(3) E3 encompasses EMC; EMI; EMP; electromagnetic radiation hazards; and the natural phenomena effects of lightning and electrostatic discharge. This E3 environment is typically created by emitters, electrical motors, and nature (for example, lightning). The following approaches may be employed to resolve E3 problems:

(a) Operational fix—operational avoidance of electromagnetic sources, elimination of particularly susceptible configurations/deployments or elimination of reliance on susceptible items, and mobilization and/or dispersion of assets to increase survivability and compound targeting difficulties.

(b) Proliferation—field the system in sufficient numbers to compensate for expected susceptibilities.

(c) Materiel solution—incorporation of physical or electronic design protection (hardening) by means of shielding, filtering, and protective circuitry. The review and analysis process should consider the merits of the various E3 tests planned, expected operational electromagnetic environment, applicability of E3 criteria and methodology, and the scope and appropriateness of the E3 measurements and tests. The mission impact of both E3 environment-induced performance and operational degradation should be analyzed. DOT&E guidelines and procedures dealing with E3 and Spectral Management (SM) can be found at http://www.hqda.army.mil/tema.

b. The DoD Policy on Operational Test and Evaluation of Information Assurance, November 1999, defines IA as "information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities." Information operations (IO) are actions taken to affect adversary information and information systems while defending one's own information and information systems.

(1) The applicable DoDDs, DoDIs, and regulations that govern IA are the Defense Acquisition Guidebook, DoDD 5200.28, and the Policy on Operational Test and Evaluation of Information Assurance. DOT&E policy guidance applies to DOT&E OT oversight systems and directs the Services to review system IA requirements, plan and develop a test strategy, conduct appropriate developmental and operational assessments, and evaluate IA vulnerabilities during OT.

(2) Widespread use of modern computer technology has led to an increasing dependence on IT that may be vulnerable to attack. IT refers to the hardware, firmware, and software used as part of a system to perform DoD information functions. This increasing dependence on IT could be a serious problem if hostile agents gain access to sensitive information or deny friendly use. Threat effects include compromise and corruption of data and disruption of operations. IA evaluation needs to be addressed throughout a system's development and testing phases, on preplanned product improvements (P3I), and for spiral development (evolutionary acquisition) to identify the IA shortfalls and to inform the users of the subsequent operational impacts. IA applies to all T&E programs for systems that are dependent on external information sources or provide information to other Army/Joint/Allied Forces systems. The survivability analyst needs to determine whether the information system under evaluation has IA susceptibilities to be concerned about and, if so, identify what can be done to protect it from the threat. For each program, the survivability analyst develops the IA risk assessment. The ARL SLAD information flow model can be used to provide data for the assessment. IA T&E will focus on how well the system under evaluation resists computer network attack or computer network exploitation methods. The analyst ensures that IA T&E issues are identified in the evaluation plans, TEMP, and test plans.

c. Nuclear, biological, and chemical (NBC) evaluation—

(1) The Defense Acquisition Guidebook requires PMs to address "instantaneous, cumulative, and residual nuclear, biological, and chemical effects" on personnel. Additionally, the Defense Acquisition Guidebook states that "design and testing will ensure that the system and crew can withstand manmade hostile environments without the crew suffering acute chronic illness, disability, or death." AR 70–75, Survivability of Army Personnel and Materiel, specifies that the U.S. Army Nuclear and Chemical Agency (USANCA) is responsible to define all NBC contamination survivability criteria for mission-essential systems and that mission essential systems and equipment will be survivable to NBC contamination. The DA-approved NBC Contamination Survivability Criteria for Army Materiel, 1995, establishes the quantitative criteria for Army materiel designed to perform mission-essential functions. Aspects of an NBC evaluation include nuclear, biological, chemical contamination survivability (NBCCS), collective protection, detector/alarm integration, decontamination and individual protective equipment storage, and system specific NBC TTPs. The NBC evaluation considers the effectiveness of material solutions and the viability of the TTPs used by the CBTDEV to mitigate the mission impacts of operations in an NBC contaminated environment.

(2) As defined in AR 70–75, NBCCS is "the capability of a system (and its crew) to withstand an NBC-contaminated environment and relevant decontamination without losing the ability to accomplish the assigned mission. A Nuclear, Biological, and Chemical contamination survivable system is hardened against NBC contamination and decontaminants, is decontaminable, and is compatible with individual protective equipment." Elements of NBCCS are hardness, decontaminability, and compatibility. Hardness is the ability of a system to withstand the damaging effects of NBC contamination and decontamination. Decontaminability is the ability of a system to be decontaminated to reduce the hazard to personnel operating, maintaining, and resupplying it. Compatibility refers to the ability of a system to be operated, maintained, and resupplied by personnel wearing the full NBC protective ensemble.

(3) Collective protection provides a contamination-free environment (for example, shelters and crew compartments). It is protection provided to a group of individuals that permits reduction of individual MOPP levels. Collective protection should be addressed for systems that provide enclosed compartments for NBC survivability of the crew.

The evaluation issues include NBC filtration capability, platform integration, and environmental equipment performance in an NBC environment.

(4) NBC agent detector and alarm systems may be incorporated into systems to alert the crew when harmful agents are present. The evaluation should address the integration of contractor-furnished and Government-furnished equipment to determine if any degradation occurs in detector performance. Analysis and testing with simulants can be used to verify the detector/alarm performance.

(5) System load plans should be examined to ensure adequacy of space and location for protective equipment. The survivability and ILS evaluations must ensure adequacy of space and location, and the capability of the crew to gain access to the protective equipment in a timely manner. HFE MANPRINT assessments and test results will establish the level of safe accessibility.

(6) The survivability analyst should consider how TTPs address mission impacts in an NBC environment. Examples of TTPs to be reviewed are decontamination procedures, operational work arounds, and operator/crew training.

(7) The NBC evaluation must consider the CBTDEV's operational mission requirements and the MATDEV's approach for system design, including geometry, materials, and functionality to meeting those requirements. The CBTDEV's operational requirements define the MP from which the mission-essential functions and tasks are determined. The evaluation should consider the aspects of NBC evaluation relative to system level integration to include analyses of applicable decontamination procedures, logistics support, and impact to life cycle cost. The survivability evaluation should consider the philosophy on which the DA Approved NBCCS Criteria for Army Materiel are based: "A Soldier crew surviving an NBC attack should be able to continue using mission-essential systems and equipment, in a full protective ensemble if necessary. When the mission permits, the systems and equipment should be capable of rapid restoration to a condition such that all operations can be continued in the lowest protective posture consistent with the mission and threat, and without long-term degradation of materiel." The criteria for hardness, decontaminability, and compatibility describe the conditions and data measurements necessary for the system evaluation.

(8) Sources of data for analysis include materials test results and databases, such as test reports and analyses from DPG, UT, and the Chemical Biological Information Analysis Center (database), MOPP IV operational test data, operator/observer feedback, and models such as the ARL's Human Research and Engineering Directorate (HRED) Improved Performance Research Integration Tool (IMPRINT). IMPRINT can be used to characterize the impact of MOPP IV conditions on task completion times. Data requirements for an NBC evaluation are as follows:

(a) MP (to determine exposure time).

(b) Selected quantifiable mission essential functions (materiel) and operation/maintenance tasks (Soldier) with associated system components.

(c) Design/material/components/system review and analysis to identify accessible and vulnerable materials and components.

(d) Chemical/biological material databases.

(e) Material susceptibility to agent/decontaminant.

(f) Specific and significant material property change (caused by agent/decontaminant).

(g) Residual agent and desorption rate after contamination and decontamination.

(h) Component/system agent testing (if existing data are not sufficient).

(i) Time to perform tasks in MOPP IV and battle dress uniform.

(j) Problems/comments noted by operators and observers.

(k) System-specific NBC TTPs from the manufacturer and PM, in conjunction with the user requirements.

d. NWE evaluation:

(1) AR 70–75 specifies that USANCA is responsible to define all nuclear survivability criteria for mission-essential systems. This regulation also states that mission-essential electronics must survive high-altitude electromagnetic pulse (HEMP). The MIL–STD–2169 specifies the classified HEMP survivability criteria. A system that must survive at a given distance from a surface or near-surface burst has a requirement to survive HEMP effects as well. System response can be categorized into two main types: the physical/structural response of exposed system components and materials to the ground burst environments of air blast and thermal radiation; and the transient or permanent change response of electronic and electrical components to the EMP and initial nuclear radiation (INR) environments. The goal is to provide the appropriate protection for the system. If a necessary fix is very costly or technically infeasible, only the chairperson of the Nuclear and Chemical Survivability Committee (the DCS, G–3) can grant a waiver (that is, relief from achieving the protection level specified in the criteria, but not relief from the requirement to be nuclear survivable).

(2) Tactical systems will not survive a direct hit from a nuclear weapon surface burst. A surface burst occurs when detonation takes place either on the ground or close enough to the ground that the fireball touches the surface. For example, the diameter of the fireball of a one-megaton weapon may be 1.7 km (1.1 mile). In this case the height of

burst must be below 0.87 km (0.54 mile) to cause a surface burst. The reference point on the ground directly below the burst is called ground zero. The criteria are based on the approach that at some distance from ground zero, depending on the weapon size and height of burst, half of the Soldiers are expected to survive well enough to be able to complete their mission. The survivability evaluation must assess the system's functionality at these tactical threat levels for the survivors. Air blast, thermal radiation, INR, and low-altitude EMP are the effects resulting from a surface or near-surface burst and occur within the first minute following detonation.

(3) HEMP results when a nuclear detonation occurs outside the earth's atmosphere. A nuclear detonation produces an electrical disturbance, which is an EMP that can cover a whole theater of operations resulting in theater-wide loss of all susceptible electronic equipment, and with no impact on Soldier survivability because humans are not susceptible to HEMP. Since HEMP occurs as a result of detonation of a nuclear warhead above 35 km, no blast, thermal radiation, or INR effects reach the ground. A "HEMP only" requirement typically applies to small systems (for example, the electronically fused round) found in large numbers throughout the theater. The system must be protected against theater-wide loss to HEMP, but localized loss of a small number of systems to blast, thermal, or radiation effects in a surface burst may be acceptable to the user, as specified in the ORD. Consequently, the surface area where unhardened equipment fails could be the size of an entire continent.

(4) Testing and analytical tools:

(a) Test Facilities. HEMP effects on a system cannot be accurately predicted by analysis because current M&S capabilities cannot adequately characterize the system's response. Thus, HEMP testing is required to provide credible data input to the survivability evaluation. DTC's WSMR, NM, and the Navy's Patuxent River Naval Air Warfare Center, MD, are facilities capable of conducting system-level HEMP tests. Also located at WSMR are the Large Blast Thermal Simulator (LBTS), Solar Thermal Facility (STF), and several facilities for testing INR effects. The LBTS simulates the blast and thermal effects associated with a nuclear weapon detonation on an integrated nuclear battlefield and is capable of varying shock overpressures and duration independently. The STF provides intense rectangular and shaped thermal pulses for simulation of the high temperature effects of nuclear weapons. For INR testing, the Fast Burst Reactor (FBR) provides neutron environments; the Linear Electron Accelerator (LINAC) and the Relativistic Electron Beam Accelerator (REBA) produce INR dose rate environments; and the Gamma Radiation and Eldorado facilities generate INR total dose environments.

(b) Models. For air blast effects the Truck model may be useful to characterize vehicle overturn, but it is not useful to predict damage to exterior mounted equipment, thermal radiation, INR, or HEMP. A model used for thermal radiation effects is the Thermal Analysis of Skins Under Load (TASL). TASL is useful for determining heat distributions across various external surfaces. The model will highlight system thermal radiation vulnerabilities. This information is important for design planning. Some limitations of TASL are that the model does not consider interfaces, layers of material, or blast effects. For INR, the Monte Carlo Adjoint Shielding Code (MASH) model can be used in T&E. It is the only USANCA-approved model for INR analysis of combat vehicle interiors. MASH provides radiation protection factors in the INR environment. The quality of the evaluation depends on a clear understanding of the system's mission, the expected nuclear environments that the system is required to survive, supporting analyses and testing, any modifications to criteria through the waiver process, and the battlefield impact of any open issues.

(5) A significant effort in nuclear survivability test design and evaluation is spent in getting all the proper information. This includes being proactive in interpreting nuclear survivability requirements, defining the scope of testing, and focusing on how the requirements can be met in a cost-effective manner. The level of detail of the evaluation depends largely on the current acquisition phase of the system. Early in the acquisition cycle, the evaluation should address plans for testing and analysis, identify any new technology that could present a risk, and provide an overview of contractor documentation on the internal process of incorporating nuclear survivable parts into the system design. Later in the acquisition cycle, the evaluation will also incorporate test data from the program/project management office and contractor. Any problems along the way should be clearly documented with the intent of having the problem resolved as early as possible. Mission impacts of any problems, risks, or shortcomings should be evaluated. The analyst and tester should recommend fixes and retesting as deemed necessary based on experience from other systems. The evaluation should address the following: procedural changes implemented, NWE specific instructions in training manuals, implications of any waivers granted, system's ability to complete its mission following exposure to the NWE, and the mission impact of any open issues. The Guide to Nuclear Survivability Evaluation, May 2000, provides guidance to assist in the planning and conduct of nuclear survivability tests and evaluations of Army systems.

e. EW evaluation—

(1) Several sources of requirements, policy, and regulations offer guidance to the analyst when planning the EW evaluation. The STAR is the source of the threat requirements. The Defense Acquisition Guidebook and AR 70–75 provide regulatory guidance.

(2) The various aspects of EW are categorized as electronic attack (EA), electronic support (ES), and electronic protect (EP). The EW considered here pertains to threat EW against U.S. systems.

(a) Electronic attack is the area of EW involving the use of electromagnetic or directed energy to attack personnel, facilities, or equipment to degrade, neutralize, or destroy enemy combat capability. EA (for example, electronic countermeasures, and jamming) can deny or disrupt sensor performance by signal denial or interference, deception, and partial or complete damage. Essentially any equipment having sensors or receivers (for example, communications systems, radar systems, and missile receivers) is susceptible to EA. Effects caused by EA include false alarms, reduced signal-to-noise ratios, false positions (range or velocity), tracking errors, damage to sensor electronics, increased signal-to-noise ratios (to deny information), and damage to human eyes. Some EA devices can permanently destroy electronic components and sensors.

(b) ES is the area of EW involving actions to intercept, detect, identify, and locate radiated electromagnetic energy sources for the purpose of immediate threat recognition and attack warning. ES provides information required for decisions involving EW operations, threat avoidance, targeting, and other tactical actions such as electronic countermeasures. This information is collected using electronic surveillance measures, electronic intelligence, radar warning receivers, laser warning receivers, and acoustic transducers.

(c) EP is the area of EW involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment of EW that degrade, neutralize, or destroy friendly combat capability. EP is a response to counter EA or ES threats. EP encompasses electronic counter-countermeasures. These techniques include increased transmitter power to "burn through" an interference source, frequency hop signal transmission, large transmit/receive bandwidths, constant false alarm rate algorithms, signal phase coding, polarization diversity, and low sidelobe antenna structure. EP also includes camouflage, concealment and deception techniques that suppress or modify visual, infrared, and acoustic, seismic, magnetic and RF signatures. EP signature techniques include use of radar absorbing materials or structure (RAM/RAS), low emissive coatings, indigenous vegetation as covering, terrain for masking (for example, increase of clutter level), decoys, obscurants, and atmospherics. All of these help to suppress or modify target signatures.

(3) ARL's SLAD is a source of expertise for system EW studies and analyses. Several Army sites exist for EW field and laboratory testing, including WSMR, NM; Fort Monmouth, NJ; and the EPG at Fort Huachuca, AZ. Test sites specifically suited for the signature aspect of EP are ATC, MD; WSMR, NM; Eglin AFB, FL; and Naval Air Weapons Station (China Lake), California. Models and simulators applicable to EW evaluation are the Modular Covert Remote EW Simulator and the Target Receiver Injection Model. Some of the models used specifically for signature evaluations are the Moderate Resolution Transmittance model that calculates atmospheric transmittance and radiance, the ACQUIRE model that calculates the probability of threat optic/electrooptic sensors acquiring a target under various environmental conditions, and the VSAT model that calculates probability of detection for top-attack and ground surveillance RF threats.

(4) The focus of the evaluation is whether the system can perform its mission in the operational EW environment specified in the STAR and the ORD. Issues applicable to the EW evaluation include system level RF vulnerabilities, performance degradation, operator workload, survivability equipment employed, operational environment, and any M&S data requirements.

f. Weapons that employ sensors (and the software logic) may be affected by obscurants, natural aerosols, and atmospheric effects that may be encountered on the battlefield. Sensors are required to perform missions in hot, basic, and cold environments, wet and dry conditions, and urban and open terrain. Sensors need to be effective in combat environments and conditions where target discrimination is difficult. Factors that impact sensor performance include clutter (natural or battle-induced), optical turbulence from hot roads and terrain, dust from moving vehicles or munitions, burning crude oil, manmade smokes, rain, snow, and fog.

(1) Several methods of testing the effects of the atmosphere and obscurants on weapon systems exist.

(a) One approach is to use the weapon system in the degraded atmospheric or obscured environment and monitor the critical performance criteria of the weapon system (for example, monitor whether the system detected the presented target, received the correct range to target, and successfully tracked the target). While performing these operations, the attenuation to the target and the atmospheric effects can be measured. In general, the technical instrumentation is used to collect data that allows for weapon system modelers to produce accurate models on the effects of the atmosphere and obscurants on system performance.

(b) The use of M&S is also useful for evaluating the atmospheric and obscurant effects on weapon system performance. The Electro-Optical Systems Atmospheric Effects Library is a library of computer models that examine the effects of atmosphere and weather. This library is managed by ARL–SLAD. The CECOM, Night Vision and Electronic Sensors Directorate, has models and databases that predict the effects of obscurants and atmospherics on night vision devices. Two of the models, ACQUIRE and FLIR92, assess the impact on thermal imagers. The U.S. Army

Missile Command Research, Development, and Engineering Center has models and databases that pertain to the effects of obscurants and atmospherics on missile systems.

(2) In order to determine the effectiveness of weapons systems using sensors, the weapons system should be tested and evaluated for performance in realistic combat environments that include some portion of these atmospheric and obscurant effects. Mission impacts of system operation in these degraded environments should be assessed.

g. AR 602–2 established Soldier survivability as the seventh domain of MANPRINT. Soldier survivability is unique to MANPRINT in that it addresses the survivability of a Soldier under combat conditions. Soldier survivability is comprised of six components: I—Reduction of Fratricide; II—Reduction of Detectability; III—Prevention of Attack; IV—Minimization of Damage; V—Minimization of Medical Injury; and VI—Reduction of Physical and Mental Fatigue. ARL's SLAD is designated as the Army lead for performing the Soldier survivability assessment on major and designated non-major systems. SLAD is supported by ARL HRED and by the U.S. Army Medical Research and AMC. HRED is responsible for the Soldier survivability assessment for the remaining non-major acquisition systems. The Soldier survivability assessment is used as input to the evaluation in the formulation of issues, measures, and data elements in the survivability T&E plans and reports.

h. System DT and evaluation will generally address system survivability to ballistic threats. Modern threats typically include either man-in-the-loop or autonomous guidance capability. As such, system survivability must consider—

(1) Acquisition avoidance (do not be seen).

(2) Hit avoidance (do not get hit if seen).

(3) Kill avoidance (minimize damage to crew or hardware given an impact or perforation by a lethal mechanism).

i. Acquisition avoidance will generally be captured under E3, EW, or obscurants evaluations. Hit avoidance may be assessed under EW or obscurants if signature suppression, modification, or spoofing are employed. Hit avoidance will be assessed under ballistic survivability if active protection mechanisms are used to physically block or degrade engagement by a threat lethal mechanism. Ballistic survivability must encompass kill avoidance measures (assuming a hit), which will include—

(1) Protection against lethal mechanism perforation.

(2) Vulnerability reduction given a threat interaction.

(3) Design for repair (to enable crew to expeditiously return to battle or remove themselves from the engagement area).

j. Major systems will be required to undergo congressionally mandated LFT&E (see app S). System survivability to ballistic effects is an intrinsic issue for LFT&E, and therefore will be addressed under LFT&E for covered systems. For non-covered systems, ballistic survivability should be addressed in the same building-block approach as identified for major systems in the LFT&E section. Specifically, modeling and testing (as necessary) will be conducted at component level, subsystem/system level, and FUSL, with a goal of identifying damage mechanisms, synergistic damage mechanisms, and crew survivability issues. Crew survivability will always be addressed if applicable. Loss of system functionality will be the primary measure of effects, with the specific criteria (mobility, firepower, and communication) being dependent on the system evaluated. Damage criteria appropriate for the system of interest will be coordinated among the user (TSM), intelligence, and evaluation communities, with ARL/SLAD having responsibility for defining the system criticalities that result in each criterion. The goal of ballistic survivability related T&E is to identify potential areas of ballistic susceptibility as early as possible in the development process, so that possible fixes can be investigated and incorporated as early as possible. Attention must be given to identifying and evaluating those portions of the system that will most affect the system functionality. At all phases of the system development, the evaluation should place emphasis on identifying possible vulnerability reduction features to provide improved survivability for both system and crew. The evaluation of ballistic survivability should include an assessment of survivability to all expected threats identified in the ORD. The STAR should also be reviewed for possible threat classes not specifically identified in the ORD.

k. Modeling and testing/experimentation play an important role in the determination and improvement of system survivability to ballistic threats and enhancement of munition lethality throughout the acquisition process. ARL/SLAD is the Army's proponent for system level ballistic vulnerability/lethality models (MUVES/Advanced Joint Effectiveness Model) that are typically used to conduct trade studies, provide war game inputs, support LFT shot selection, and conduct LFT pre-shot predictions. Other engineering level models can also come into play to address specific damage mechanism or vulnerability reduction issues. Testing and experimentation complement efforts to develop modeling inputs, validate model results and to demonstrate vulnerability reduction design techniques.

I–6. Summary survivability evaluation process

System evaluation is a team process and a survivability analyst will be part of a system team and a T&E WIPT. These teams provide avenues to technical support. In addition to support from team members, support in the areas of survivability is available from other Government agencies, contractors, other survivability analysts, and the analyst's supervisor. The survivability analyst works in an environment of change. The nature of the design, development, and production processes of systems dictates that documents will require continual updates. Survivability requirements are continuously changed and updated due to the impact of emerging technology, new threats, and increasing dependence on global information systems. The analyst should proactively review the regulations, military standards, test procedures, policies, ORDs, and system descriptions in anticipation of these changes.

Appendix J

Live Fire Vulnerability/Lethality Issue: System Evaluation Considerations

J–1. Overview of live fire

a. Title 10, United States Code, mandates that major weapon system and munitions programs, as well as product improvements to those programs that are likely to significantly affect the vulnerability or lethality of those programs (respectively) undergo a realistic LFT&E program. This section provides guidelines for test design and evaluation planning for LFT&E programs. It also presents the basis for determining whether a LFT&E program is required for a given system, and describes the key steps in developing an adequate and acceptable LFT&E strategy, including the role of M&S in the LFT&E process. Specific guidance on the planning, execution, reporting of live fire tests is provided in chapter 6 and appendix S.

b. LFT&E is necessary because it is the law; but, more importantly, because it is cost effective and smart testing. A realistic LFT&E building block program represents the best alternative to "actual" combat in assessing the system's performance. However, with the lack of actual combat data must come a disciplined and realistic approach to assessing the vulnerability and lethality of our weapon systems. The FUSL LFT component of the LFT&E program provides the means for assessing the synergistic effects of system component integration and of selected damage mechanisms. A well-planned and well-structured LFT&E program reduces the potential for "surprises" before that system's arrival on the battlefield.

c. An active, well-planned, well-managed, and well-executed LFT&E program is essential to understanding system vulnerability/lethality (V/L) and will be an essential element of the information supporting decisions regarding the acquisition of materiel as well as the development of doctrine, plans, and JMEMs for its proper operational employment. When properly structured and scheduled, the LFT&E program will enable design changes resulting from that testing and analysis to be incorporated into the system at the earliest possible date and reduce the need for expensive retrofit programs.

d. Figure J–1 illustrates the basic elements of the overall LFT&E process from initial strategy definition to the writing of the final T&E reports. While the details of each element of this overall process must be decided on a case-by-case basis, this guidance presents the general approaches and lessons learned from initial LFT&E programs that have proven successful and that should prove beneficial to those individuals involved in future LFT&E programs.

J–2. Objective of live fire test and evaluation

a. The LFT&E program supports a timely and thorough assessment of the vulnerability/lethality of a system as it progresses through its development and subsequent production phases. It should demonstrate the ability of the weapon system or munition to provide battle resilient survivability or lethality and provide insights into the principal damage mechanisms and failure modes occurring as a result of the munition/target interaction and into techniques for reducing personnel casualties or enhancing system survivability/lethality. These insights will mature during the course of the system's LFT&E program. Data will emerge that will identify specific failure modes and damage mechanisms. The data can be used to support cost effectiveness tradeoffs to predict the optimal "mix" of vulnerability reduction/lethality enhancement measures early (prior to MS B) in the acquisition cycle (see the Defense Acquisition Guidebook).

b. The primary emphasis of LFT&E is on realistic combat conditions testing as a source of personnel casualty, vulnerability, and lethality information to ensure potential design flaws are identified and corrected before FRP. The LFT&E program should assess a system's vulnerability/lethality performance relative to the expected spectrum of battlefield threats; it is not constrained to addressing specific design performance goals or threats. However, LFT&E by itself is not a basis for the decision to transition to FRP; many other factors must be considered in arriving at this decision. Additionally, LFT&E will provide insights into how to enhance the survivability and/or lethality of similar or future systems and provide a mechanism for gaining insights into the adequacy of vulnerability/lethality assessment techniques and supporting databases. LFT&E should exploit opportunities to assess the capabilities of battle damage assessment and repair to further system survivability.

J–3. Background of live fire test and evaluation

The genesis of LFT began in the early 1980s as the outgrowth of perceived needs by two separate groups. First, the vulnerability/lethality assessment community was concerned that the technological viability of their assessment techniques was becoming increasingly tenuous. They were relying more and more on questionable extrapolation of existing databases (rapid advances in technology over the past two decades had simply made many of these databases outdated and inapplicable). Due to the increasing complexity of foreign and domestic weapon systems and of the munition/target interaction, assessment techniques demand a strong tie to empirical databases including those based

on firings against full-up targets. Staff personnel within Congress, the OSD, and HQDA were concerned that testing programs were ignoring the realities of war and were not providing a realistic and rigorous assessment of the likely performance of these systems in combat. They felt that program decisions were too dependent on modeling and component testing and that full-up LFT was needed to judge how well these systems—and the crew who operated them—would survive on the modern battlefield.

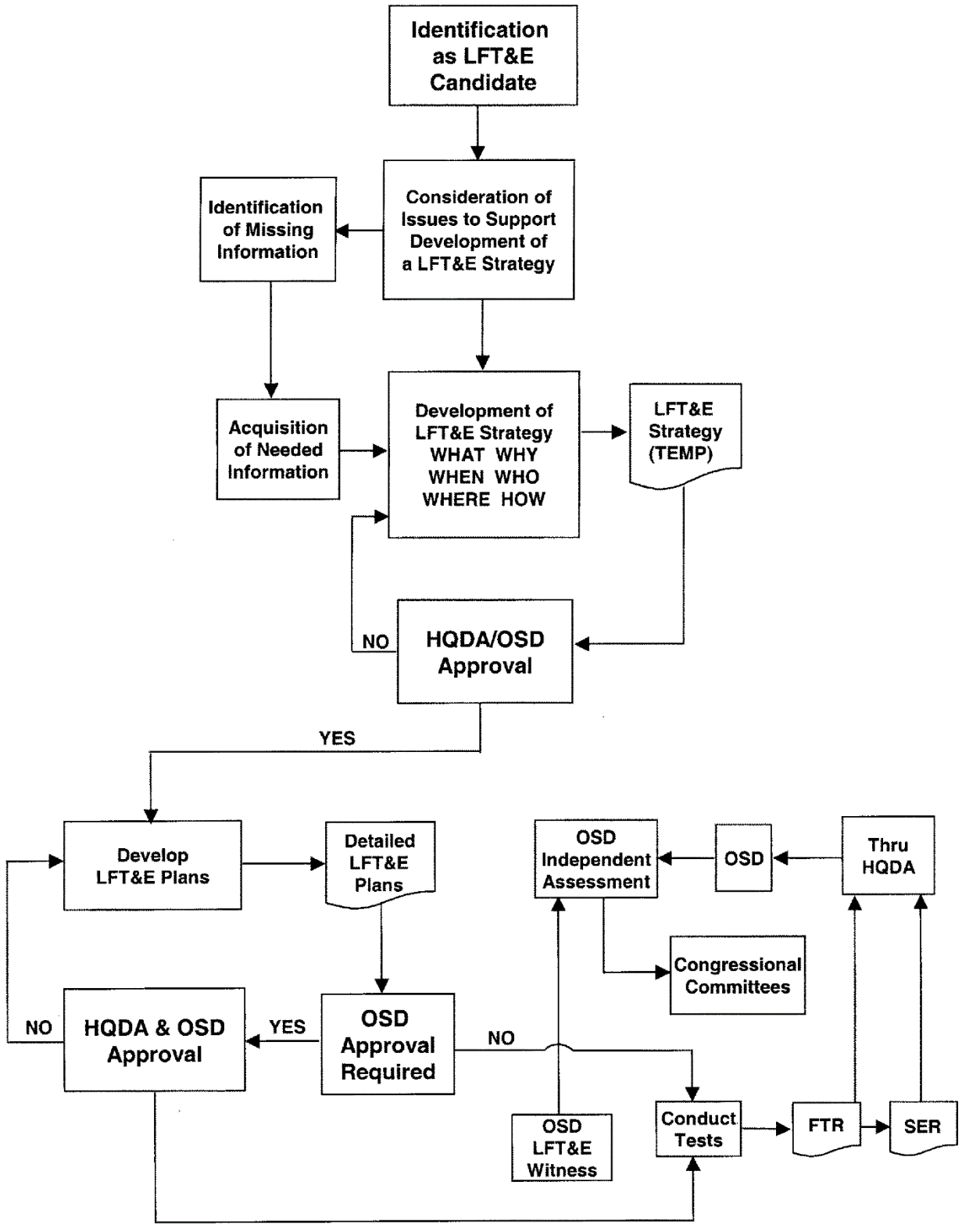


Figure J–1. Overview of the live fire test and evaluation process

a. The need for full-up testing led to the establishment of the Joint Live Fire (JLF) Program in March 1984. The JLF Program was and continues to be sponsored by OSD as a joint test initiative. The JLF Program is chartered to assess the vulnerabilities and lethalities of fielded conventional U.S. ground systems and aircraft. Army systems initially included in the JLF Program were the Bradley Fighting Vehicle System, the Abrams Tank, and the M113 Family of Vehicles. Because of differences in the philosophic approach to LFT between the Army and OSD (the building-block approach versus large scale full-up testing) and the Army's desire to accelerate the testing of these systems, the Army subsequently requested and received permission from OSD to withdraw the Bradley, Abrams, and M113 systems from the JLF Program. The Army agreed to fund the cost of the LFT programs for these systems and to provide OSD open access to test planning, test conduct, and test results. This series of LFTs was known as Army LFT and was completed in 1988.

b. The need for LFT led Congress to mandate such testing for major weapon system and munition programs through a series of amendments to Title 10, USC, in the FY86 through FY94 Department of Defense (DoD) Authorization Acts and in the Federal Acquisition Streamlining Act of 1994. Table J–1 presents a comparison of the primary features and differences among the JLF, the Army live fire, and the congressionally legislated LFT&E programs. The remainder of this pamphlet discusses the requirements and strategies applicable only to congressionally legislated LFT&E programs.

Table J–1
Comparison of joint live fire, Army live fire, and live fire test and evaluation programs required by Title 10, United States Code

Joint Live Fire	Army Live Fire	Title 10, USC
Chartered FY84	Legislated/Chartered	Legislated FY86–FY94
Multi-Service	Army only	Individual/Multi-Service
OSD funded	Army funded	Service funded
Fielded systems	Bradley, Abrams, M113 Family	Developmental systems/PIPs
Vulnerability/lethality	Vulnerability	Vulnerability/lethality
Armor/anti-armor, aircraft	Armor	Air, land, sea systems
Test event oriented	Test event oriented	Milestone oriented
OSD oversight	OSD oversight	OSD oversight

J–4. Live fire test and evaluation legislation

The FY86 and FY87 DoD Authorization Acts amended by 10 USC 139 require LFT&E before proceeding BLRIP. Specifically, the FY86 legislation requires side-by-side vulnerability LFT&E if a wheeled or tracked armored vehicle is to replace an existing vehicle; the FY87 legislation requires LFT&E for all covered systems and major munition and missile programs. The FY88–89 DoD Authorization Act amended Title 10 to include a LFT&E requirement for product improvements to major systems (that is, system changes (modifications or upgrades)). The FY90–91 Act requires DoD to report results of LFT before a system enters FRP and also acknowledges that procurement funds can be reprogrammed to support LFT&E programs (such funding will not exceed one-third of one percent of the total program cost). The FY94 DoD Authorization Act eliminates redundant sections of Section 139 of Title 10 including the requirement to conduct comparison testing with existing vehicles being replaced. The Federal Acquisition Streamlining Act of 1994 transfers oversight of live fire testing from the Office of the Deputy Director, Defense Research and Engineering (Test and Evaluation) to the DOT&E, OSD.

a. To summarize, the current legislation requires that the Secretary of Defense provide that—

(1) A covered system not proceed beyond LRIP until realistic survivability testing is completed.

(2) A major munition or missile program not proceed beyond LRIP until realistic lethality testing is completed.

(3) A covered PIP not proceed beyond LRIP until realistic survivability/lethality testing is completed.

b. The legislation states that the costs of all survivability/lethality testing will be paid from funds available for the system being tested. The legislation also allows the Secretary of Defense to waive the requirement for survivability/lethality testing in time of war or if the Secretary certifies to Congress, before the system enters engineering and manufacturing development, that LFT of the system would be unreasonably expensive and impractical. Per DoDI 5000.02, all acquisition programs, excluding highly classified programs, will be placed into one of three categories: ACAT I, ACAT II, or ACAT III. ACAT I and ACAT II programs are MDAPs and major programs, respectively, and, if they

are covered systems or a munition/missile system, will have a LFT&E requirement. Non-major (ACAT III) munition/missile programs may have a LFT&E requirement if they meet the one million round production requirement.

J–5. Requirement for live fire test and evaluation

Figure J–2 provides a flow chart to assist in determining a system's LFT&E requirement. This flow chart addresses both new systems and system changes (modifications, upgrades, or follow-on blocks) to existing systems. Specific situations (for example, the LFT&E requirements for changes to existing systems that have undergone LFT&E) must be addressed on a case-by-case basis. If a system meets the LFT&E dollar or quantity criteria or if a system change provides a significant vulnerability/lethality effect, the system has a LFT&E requirement. The degree of LFT&E needs to be addressed in a comprehensive LFT&E strategy, incorporated into the appropriate documentation, and provided to the Army leadership for guidance and approval. Per DoDI 5000.02, a system's proposed acquisition strategy and evaluation strategy developed during Pre-Systems Acquisition (Concept and Technology Development) include LFT&E testing requirements in addition to DT, OT, and System Evaluation. Army policy requires a system's LFT&E requirement be identified to the U.S. Army TEMA and a mature LFT&E strategy and resource requirements be included in the Milestone B TEMP (see the Defense Acquisition Guidebook).

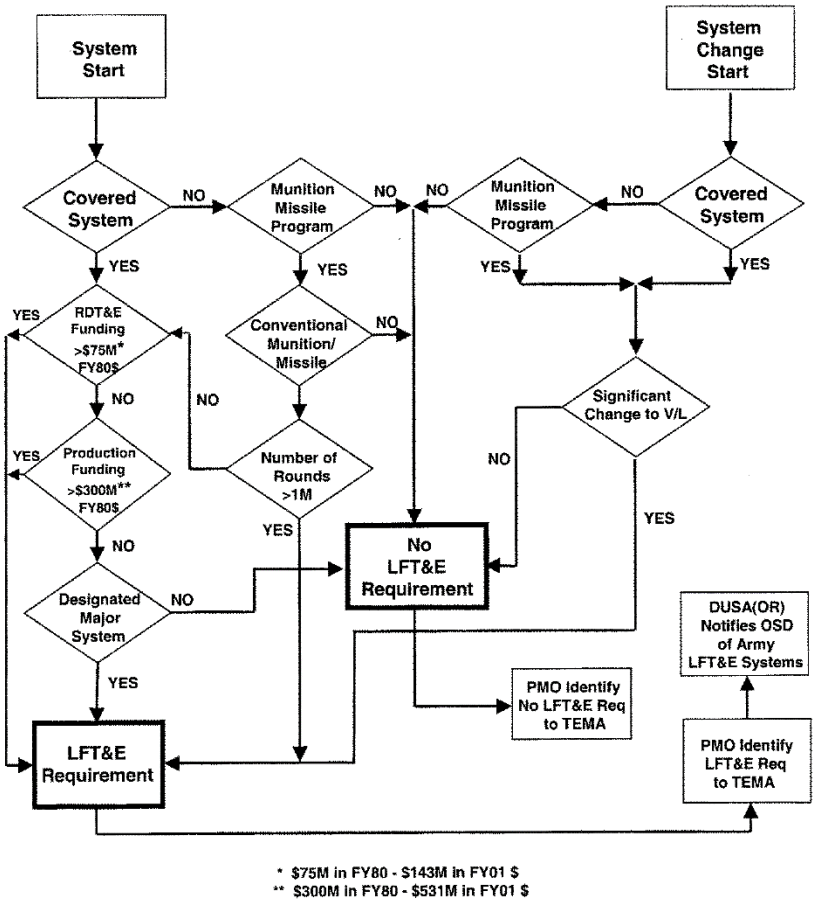


Figure J–2. Live fire test and evaluation requirements flow chart

J–6. Keys to success

The LFT&E program has and will continue to be one of the most complex and high-visibility T&E phases during weapon system development. It requires proper planning, resourcing, testing, evaluation, and coordination to ensure that critical vulnerability/lethality issues are effectively and adequately addressed and that the congressional mandate is satisfied. Based on the experience gained during previous Army LFT Programs, a number of "keys to success" have been identified that should be useful for future LFT&E programs. These keys include—

a. Integration into the test and evaluation process. The requirements of LFT&E are comparable to those of any T&E program. The T&E WIPT is supported by the LFT&E WIPT, a subgroup formed to coordinate LFT&E planning activities. The LFT&E WIPT is chaired by the system evaluator.

b. Early planning. The resource demands, plus the review and approval process, for LFT&E make early planning absolutely essential. Early identification of the critical vulnerability and/or lethality issues, the LFT&E strategy, the test resource requirements, test limitations, and inclusion in the TEMP are necessary to provide:

(1) HQDA/OSD with an understanding of the basic strategy and the adequacy of planned testing, evaluation, and resources.

(2) The PM with an understanding of the resources required, including the system hardware and threat or threat surrogate requirements, many of which require long lead times to procure or develop.

c. Building-block approach. The key to understanding a given munition/target interaction is an understanding of the underlying phenomenology. These insights can often be gained and many critical issues addressed through component and/or sub-system level T&E. Thus, the most cost effective and efficient approach to LFT is a building-block approach. Using such an approach, a development program would progress from early component level T&E, to subsystem/system level T&E, and culminate in a limited series of FUSL live fire tests. These firings address personnel casualty, the synergisms of various damage mechanisms, and critical system vulnerability/lethality issues that can only be answered through FUSL LFT&E. The building-block approach provides the earliest possible understanding of the munition/target interaction phenomena during the development process and enables required fixes to identified problems be incorporated at the earliest possible date. This approach also affords the MATDEV with a stepwise approach to acquire test information in the system design process. Evaluating the system's design for incorporating vulnerability reduction features early allows the MATDEV to evaluate alternatives to providing combat survivable systems to the user.

d. Live fire test and evaluation working-level integrated product team. The complexity of LFT&E programs requires that a broad range of technical, programmatic, and management expertise be brought together for the planning, execution, and reporting of that program. A matrix team approach has been found to be the most effective and efficient approach in previous LFT&E efforts for bringing this diverse set of expertise and activities together and ensuring a coordinated and credible LFT&E program. Thus, successful execution of a LFT&E program demands the early recognition of the need for, the solicitation of, the support of, and the continuous involvement of all necessary activities. Principal team members typically include the system developer, CBTDEV, system evaluators, vulnerability/lethality analysts, testers, medical community, intelligence community, and system contractor (as required). DOT&E and DUSA (OR) are invited to provide members since these offices have oversight responsibilities. Generally, this matrix team will remain in existence throughout the LFT&E program and should be organized as a separate working group under the T&E WIPT. Membership may be expanded or modified to include user representatives and others as required (for example, for vulnerability programs involving ground vehicles and air platforms, the Battlefield Damage Assessment and Repair (BDAR) Executive Agent may be included) and as the program evolves.

e. Live fire test and evaluation discipline. Because of the high visibility of LFT&E programs and HQDA and DOT&E approval of selected LFT&E documents, the LFT&E process must assure strict adherence to HQDA and DOT&E approved documents or obtain approval of changes by HQDA and DOT&E. Test discipline is discussed in greater detail in chapter 6.

J–7. Roadmap to live testing and evaluation

The development and subsequent approval of the LFT&E strategy is a critical step in the overall LFT&E process. The LFT&E strategy is a documented concept that describes who, what, why, when, where, and how the LFT&E requirements for a given system will be satisfied. Just as a system's acquisition strategy outlines the top level approach for the overall system acquisition, the LFT&E strategy provides the top level description of the LFT&E portion of the system's T&E strategy and is an integral part of the TEMP. Once approved, the LFT&E strategy provides the basic roadmap for what vulnerability/lethality testing and evaluation has to be conducted before transitioning to FRP. While the details of the LFT&E strategy will vary from system-to-system, this chapter attempts to provide the general details necessary for the development of an adequate and credible LFT&E strategy. Development of the LFT&E strategy requires an understanding of both the system's acquisition strategy and the overall T&E process.

J–8. Events schedule

Figure J–3 depicts where the elements of the required vulnerability/lethality assessment and the LFT&E program fall within the materiel acquisition process as outlined in DoDI 5000.02. Table J–2 presents an outline schedule of LFT&E events that, if followed, will result in a timely and effectively executed LFT&E program. The schedule for the EDP, final test report, and SER are mandated requirements.

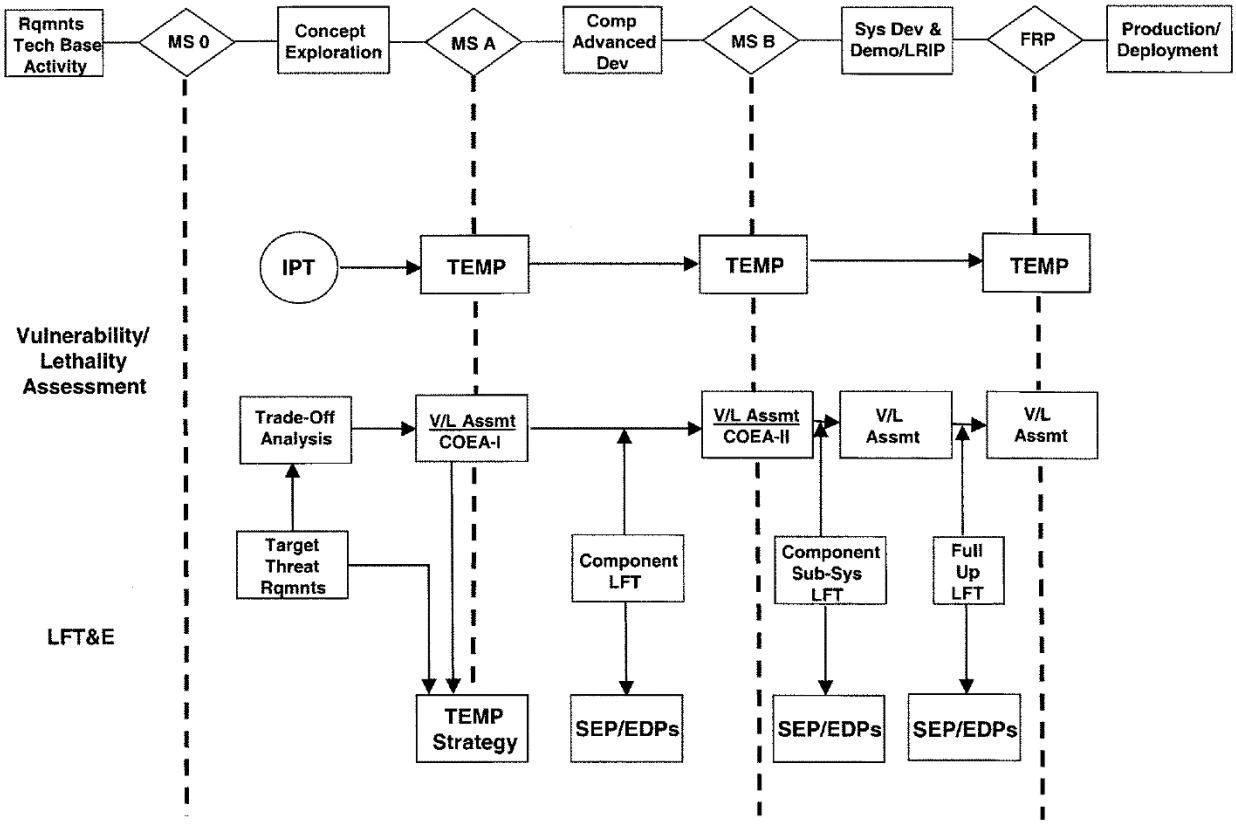


Figure J–3. Conceptual live fire test and evaluation approach to systems acquisition process

J–9. Live fire in the test and evaluation process

Live fire tests may consist of component, subsystem, or system level tests in addition to the FUSL tests of system vulnerability and lethality. The FUSL live fire testing is the testing that fully satisfies the statutory requirement for "realistic survivability testing" or "realistic lethality testing" (as defined in Title 10, USC) and is required, with OSD oversight, before a program may enter FRP. The LFT&E program examines the full spectrum of battlefield threats, to include overmatching threats, as opposed to the design level threats. The LFT&E program includes all vulnerability/lethality T&E phases and associated modeling and analysis efforts that support the live fire evaluation. Resource and schedule constraints and the stochastic nature of the FUSL LFTs generally limit the scope of these tests to a demonstration of system vulnerability and lethality.

Table J–2
Live fire test and evaluation event

Schedule	Live fire test and evaluation event	Lead	Lead for resources
Pre-MS A	Working Group Formation	ATEC (AEC)	N/A
MS A	Initial TEMP Input	ATEC (AEC)	PM
MS B	Detailed TEMP Input	ATEC (AEC)	PM
E–180* E–60*	EDP submittal to DUSA (OR) Submittal to DUSA (OR): EDP DTP Pre-shot prediction report BDAR support plan, if required**	ATEC (AEC) ATEC (AEC) Tester ARL/SLAD or SMDC BDAR Executive Agent	N/A N/A
E	Live Fire Test	Tester	PM

Table J–2
Live fire test and evaluation event—Continued

E+60	Final test report	Tester	N/A
E+110	SER for FRP Decision	ATEC (AEC)	N/A
E+120	Final test report and SER to OSD	DUSA (OR)	N/A
E+180	Model comparison report	SLAD	N/A

Notes:
* These scheduling guidelines pertain to the FUSL LFT&E phase. Timelines may vary for other LFT&E phases.
** For BDAR support plan and report requirements, see system LFT&E strategy.

J–10. Elements

System developmental tests and evaluations typically address the following factors: firepower (lethality is an element); survivability (vulnerability is an element); performance; safety; RAM and durability; MANPRINT; ILS; and software. The LFT&E program addresses elements of firepower and survivability, which are compared/contrasted in table J–3.

Table J–3
Elements of firepower and survivability

Firepower	Survivability
Ability to acquire targets	Avoid or reduce acquisition
Ability to hit an acquired target	Avoid or reduce being hit given an acquisition
Ability to kill a target given a hit (lethality)*	Avoid or reduce being killed given a hit (vulnerability)*
Ability to perforate or breach target*	Protect against lethal mechanisms*
Ability to do significant damage to the target*	Limit damage to crew and hardware*
Rate of aimed fire	Design for expedient repair of combat damage*

Notes:
* Focus of LFT&E.

J–11. Sub-elements

Both lethality and vulnerability LFT&E address system performance given a munition effect. At the sub-element level, lethality LFT&E addresses both the ability to perforate or breach the target and to do significant damage to the target. Vulnerability LFT&E addresses both being protected against lethal mechanisms and minimizing damage to the crew and hardware given an impact or breach by a lethal mechanism. In addition, vulnerability LFT&E addresses recoverability from combat damage (another element of survivability).

J–12. Differences between vulnerability and lethality

There are several subtle differences in vulnerability versus lethality LFT&E. Vulnerability LFT&E must address crew, hardware (excluding crew), and system (crew and hardware) vulnerability for threats and impact conditions that the system may not be designed to protect against and for threats and impact conditions that the system is not designed to protect against but could encounter on the battlefield. In lethality LFT&E, the FUSL LFT may focus on demonstrating lethality against the selected threat systems for areas that have the greatest protection and/or where differences between competing munitions are expected (not only areas of greatest protection), relying more heavily on modeling/analysis to evaluate lethality against other target areas or other targets. For example, a new munition may not be able to breach the area of greatest protection on the threat; however, for areas that it can breach, the damaging effects (for example, probability of kill given a hit (Pk/h)) may be significantly greater than the munition being replaced.

J–13. Developing the live fire test and evaluation strategy

The LFT&E strategy is the most important element of the LFT&E process. It should be prepared and approved as early as possible in the acquisition cycle. The system evaluator has the lead for preparing and obtaining approval for the strategy in coordination with T&E WIPT. The DUSA (OR) approves the strategy for the Army before it is sent (via the TEMP) to the DOT&E for OSD approval. If consensus on the scope of the LFT&E cannot be reached, or if program constraints limit compliance with required reporting dates, these issues will be raised to the DUSA (OR) for

resolution. The strategy is the foundation of the LFT&E section of the TEMP and all subsequent planning documents (the SEP, EDP, the Pre-Shot Prediction Report, and the DTP). The strategy should be detailed enough to adequately project resource requirements, schedules for major T&E efforts, and trigger long lead time planning, procurement of threats/surrogates, and modeling.

J–14. Background information necessary to develop the strategy

The first step in preparing a strategy is to do the necessary research to—

a. Understand the technical and operational characteristics of the concepts, technology, and requirements for the system being developed and how they differ from the system being replaced (where appropriate).

b. Develop a rationale for which threats are to be considered in the LFT&E. The rationale should be based upon a review of the STAR, the densities of the various classes of threat weapons and countermeasures in organizations likely to be encountered, and the frequency that various threats kill or are killed by the system from force effectiveness analyses supporting program decisions or planning studies. An accepted rationale from an approved vulnerability LFT&E plan was to break threats into major and minor threats. A major threat was either one that killed or reduced the effectiveness of a large percentage of the systems in the force effectiveness evaluation or had a high density in the force; all others were considered minor threats. Most of the shots fired in vulnerability LFT&E should be with major threats. The rationale for lethality LFT&E should be based on the threat that is driving the design (usually the most difficult target to kill given a hit).

c. Identify, for lethality LFT&E, threat target requirements and availability. The PMs provide funding and acquire targets for lethality LFT&E.

J–15. Define the critical issues

Having completed the homework on the developmental system, the next step in developing a strategy is to define the critical evaluation issues. Critical issues are developed to address overall system vulnerability and/or lethality. Testing should provide valuable inputs and a basis for refinement and calibration of vulnerability and lethality models. Critical issues vary for vulnerability and lethality and generally should address the following:

a. Vulnerability live fire test and evaluation.

(1) Crew, hardware, and system vulnerability.

(2) Known vulnerabilities and vulnerability reduction techniques (for example, increased ballistic protection, less sensitive munitions, and redundant components).

(3) Potential vulnerability reduction techniques.

(4) Processes, provisioning, repair times, and training required for BDAR.

b. Lethality live fire test and evaluation. Testing should provide valuable inputs and a basis for refinement and calibration of lethality models and databases. It should also demonstrate the following:

(1) Ability to perforate or breach the protection of the threat system.

(2) Ability to significantly degrade the combat/mission functions of threat systems given a breach.

(3) Potential lethality improvements.

J–16. Finalization of the evaluation process

During the examination of the vulnerability/lethality of the system being developed and the defining of the critical issues, the process by which the LFT&E results will be evaluated is formulated. The next step after the strategy development is finalizing the evaluation process and articulating the details of this process in the SEP and LFT&E EDP. (See para 6–28*d*.) The evaluation must crosswalk all vulnerability/lethality testing and complementary modeling and assessment with LFT&E issues. Some aspects of the evaluation process that must be examined in the development of the LFT&E strategy are—

a. Consideration of the use of M&S to address evaluation issues pertaining to system vulnerability or lethality, crew casualties, and logistics supportability.

b. Building block level vulnerability tests are planned to assess the ability of the protective system of the item under test (for example, armor and optics) to withstand impacts by threat missiles and projectiles, and to examine the ability of critical components (for example, ammunition compartments) to withstand damage from a threat warhead or projectile that breaches the protective system. During the System Development and Demonstration Phase, the LFTs will focus on component/subsystem level to address vulnerability issues and upgrade and develop the system vulnerability model. The FUSL vulnerability LFT conducted against a full-up (combat-loaded) production or production representative system is generally the last in the series of LFTs conducted.

c. Lethality LFTs must be planned to assess the ability of the system to damage critical components and the crew. During the development and demonstration, the tests will usually focus on the warhead or penetrator's ability to breach

the threat target's protective system. During PQT, impact conditions will be firmly established for the missile or projectile and the ability of the warhead or penetrator to breach the threat target's protective system will be refined. The FUSL lethality LFT is the last LFT phase and is conducted against a full-up (combat loaded) threat target. However, it is recognized that the extent of target functionality and application of combat load may be impacted by availability of assets and specific T&E requirements. However, it is unlikely that the desired threat target will be available. (The Army develops munitions/missiles to "defeat" projected threats that in most cases have not been fielded.) Therefore, FUSL lethality LFTs must use the best available threat targets. The scarcity of lethality LFT targets and their cost may dictate that these targets not be fully combat-loaded with live munitions to preclude a catastrophic loss.

d. Vulnerability models are also used to estimate the spare parts and time required to repair combat damaged components. FUSL vulnerability LFTs provide valuable inputs for refining these estimates. In addition, rapidly returning damaged systems to battle requires being able to accurately assess the damage and apply field expedient repairs. Again, FUSL vulnerability LFTs provide both valuable training and opportunities for TRADOC to refine and develop field expedient repair methods and to identify tools and materials required to execute these repairs.

J–17. Identification of the threat target and munition requirements

An integral part of LFT&E strategy development is the identification of the threat target (lethality LFT) and munition (vulnerability LFT) requirements. These requirements need to be identified early on in the acquisition cycle to allow for possible long lead times for procurement. It is very likely that some of the required threat munitions will not be available for LFT. It is also likely that intelligence data on some munitions may be limited. Therefore, LFTs may be conducted using threat munitions based upon postulated technology options derived from intelligence assessments. This will require surrogates in lieu of "real" threats. The rationale for threat surrogate selection, and the DCS, G–2 approval of surrogate threat munitions, must be detailed in the EDP.

J–18. Rationale for selecting surrogate threat projectiles

The rationale for selecting surrogate threat projectiles for vulnerability LFTs is to match physical and performance characteristics of the projected threat. For kinetic energy projectiles, penetration into rolled homogeneous armor (RHA); muzzle velocity and impact velocity; and penetrator material, length, and diameter are typical key parameters. For shaped charge warheads, penetration into RHA; impact velocity; and warhead diameter, explosive type, and material are typical parameters. Availability and cost of surrogate projectiles may also drive the selection. Typically, U.S. projectiles and warheads will be selected as surrogates. The projectiles and warheads selected as threat surrogates must be submitted, along with the supporting rationale, by ATEC (AEC) to the DCS, G–2 for approval.

J–19. Shot selection process (full-up, system level live fire testing phase)

In order to provide the appropriate information required to address critical LFT&E issues, the attack conditions and the munition/target impact location (that is, shotline) must be identified for each shot. The shotline selection methodology that will be used is described in the LFT&E Strategy, whereas the specific shotlines selected and the rationale for their selection must be included in the EDP. There are two types of shots: engineering and random. Engineering shots provide information and data to address specific vulnerability or lethality issues for a specific threat. Random shots are selected from the combat distribution of impact conditions (direction, location, and range) for the threats of interest. The minimum number of engineering shots should be selected first to address the vulnerability and/or lethality critical issues. Next, the number of random shots required for each threat weapon should be selected. Random shots should be reviewed to determine if any engineering shots are duplicated or if a critical issue is satisfied by a random shot. Those engineering shots duplicated by a random shot should be eliminated.

J–20. Shot selection constraints and guidance

a. Questions that need to be answered in order to select the number and types of LFT&E shots are as follows:

(1) What are the characteristics of the system being developed?
(2) What is the current state of knowledge about system vulnerability or lethality?
(3) What are the critical issues?
(4) What are the threats?
(5) What are the physical and performance characteristics of the threats?
(6) If threat munitions/targets are not available, then what is the rationale for threat munition/target surrogates?
(7) What are the program and test constraints?
(8) Has any high level guidance been provided?

b. The first five questions have been discussed previously. The last three questions are discussed below to provide an outline of the parameters to be considered in selecting LFT&E shots.

c. Ideally, system program schedules and funding should be developed based upon detailed LFT&E planning; however, early in the acquisition cycle, the level of planning is usually unrefined and decisions are made that lock in schedules and funding levels. The LFT&E program should be planned independent of constraints and then efforts must be made in developing and approving the strategy to obtain relief from schedule and resource constraints. The most likely outcome of this process is compromise and trying to work out strategies that meet the spirit and intent of the law within existing or modified constraints.

d. Test facilities may constrain LFTs. There may be a need for new facilities or instrumentation. Time and money may not be sufficient to develop new facilities. In addition, there may be competing demands for LFT facilities for concurrent system developments.

e. High-level guidance is frequently provided on the number or percentage of random shots, threats to be included, conditions to be fired, test design and statistical tests to be used in the evaluation (for example, pair-wise comparison using the Sign Test), vulnerability or lethality issues to be assessed, and test methods. This guidance must be taken into account explicitly in developing the strategy. If the guidance cannot be accommodated, then the rationale for not addressing it must be presented.

f. The other major constraints are the availability of threat projectiles for vulnerability tests and threat targets for lethality tests. For developmental systems, it is almost a certainty that threat projectiles and threat targets will not be available or, if they are, that they will be available in very limited quantities. Developing a rationale for selected threats or surrogates that is practical (in terms of availability and cost) is important, especially for lethality LFT&E.

J–21. Parameter selection and specification

a. For each munition/target combination, the following parameters must be selected and specified: range, angle of attack, and point of impact. For engineering shots, the procedure for selecting these parameters is straightforward; that is, select the threat and the required parameters to address a specific vulnerability/lethality issue. For random shots, the procedure is based on random selections from battlefield distributions of the appropriate parameters. The Board on Army Science and Technology developed a methodology for selecting random shots for the Bradley Live Fire Vulnerability Test. The Board on Army Science and Technology methodology was revised for the Abrams Vulnerability LFT to better distribute the random shots over the entire vehicle when the sample size was small. The revised random shot methodology was reviewed and approved by members of the Board on Army Science and Technology. This methodology should be considered for future LFT&E programs. The random sampling parameters for direct fire threats versus an armored target are as follows:

(1) Posture (attack or defense).
(2) Range (based upon attack or defense posture).
(3) Angle of attack (stratified into equal probability intervals to ensure sampling over all possible attack angles with small sample sizes).
(4) Target side (left or right).
(5) Hull or turret.
(6) Horizontal dispersion.
(7) Direction of horizontal dispersion (left or right).
(8) Vertical dispersion.
(9) Direction of vertical dispersion (up or down).

b. The sampling parameters for random shot selection must be modified as a function of weapon class (direct fire weapons, indirect fire and top attack weapons, mines, and so forth.). For example, none of the preceding parameters apply for pressure-activated mines. For pressure-activated mines, the sampling parameters would include right or left track and the location under the track.

J–22. Exclusion rules

Exclusion rules may also be established for rejecting random shotline draws. Typically, these exclusion rules for armored targets reject shots that—

a. Do not impact turret or hull armor.
b. Are a repeat of another random shotline.
c. Are a repeat of a previous full-up vehicle shot.
d. Are expected to result in insignificant damage.

J–23. Live fire test and evaluation and the test and evaluation master plan

a. The TEMP is the basic planning document for all T&E and is the document by which the Army formally coordinates and approves the LFT&E strategy for a given system and communicates that strategy to OSD. The preparation

and processing of TEMPs is conducted under the auspices of the T&E WIPT. (See chap 3 for guidance concerning TEMP procedures and formats to be followed in the TEMP preparation.) The T&E WIPT provides the forum to effect coordination and resolve problems in the LFT&E process. A separate LFT&E WIPT under the T&E WIPT is formed to prepare the LFT&E strategy and the LFT&E input to the TEMP. This smaller group (chaired by the system evaluator), combined with the classified nature of LFT&E, enables these items to be developed in a more timely and efficient manner. Additionally, the LFT&E WIPT may assist in any required briefings of the LFT&E strategy to HQDA and OSD.

b. The TEMP (Part IV, Operational Test and Evaluation, paragraph d, Live Fire Test and Evaluation) will contain the LFT&E strategy for the program throughout its materiel acquisition process. The TEMP summarizes what, why, who, where, when, and how the LFT&E issues will be tested and evaluated. All LFT&E that impacts on program decisions will be outlined in the TEMP. Specific items to be addressed in the TEMP are discussed in chapter 3 of this pamphlet. For LFT&E, the TEMP—

(1) Shows the relationship of the LFT&E issues to the required technical and operational characteristics.

(2) Describes the critical vulnerability/lethality issues and evaluation criteria.

(3) Outlines the planned LFT&E; discusses the amount and type of LFT&E that will be performed to support each program decision point.

(4) Describes the shot selection process.

(5) Includes a LFT&E planning matrix covering the tests in the strategy, their schedules, the issues they will address, and which planning documents will be proposed for submission to DOT&E for approval or for review and comment.

(6) Indicates where schedule, resource, or budget constraints may impact the adequacy of planned LFT&E.

(7) Describes the M&S strategy and VV&A.

(8) Identifies LFT&E resource requirements (including test articles instrumentation that must be acquired).

J–24. Strategy briefing to the Deputy Under Secretary of the Army (Operations Research)

Since the LFT&E strategy is part of the TEMP, the review and approval process established for the TEMP (see chap 3) necessarily applies to the LFT&E strategy. ATEC (AEC), in coordination with the T&E WIPT, develops the LFT&E strategy and incorporates it into the TEMP. On completion of initial coordination, but before formal TEMP submission to HQDA, it is advisable to brief the LFT&E strategy to the DUSA (OR) to solicit initial guidance/agreement in principle on the proposal. Any acquisition category program with an LFT&E requirement is necessarily on the OSD oversight list (even if just for LFT&E purposes), and thus such TEMPs must be submitted to HQDA for approval before submission to OSD (see chap 3).

J–25. Live fire test and evaluation waiver

The LFT&E legislation contains a provision allowing the Secretary of Defense to waive the requirement for full-up LFT&E if the Secretary of Defense certifies to Congress that such LFT&E would be unreasonably expensive and impractical. In time of war or mobilization, the President may suspend the LFT&E requirement.

a. A request for waiver must be submitted and approved before the Milestone B decision. The review and approval process (per HQDA memorandum) for waivers is as follows:

(1) The request for waiver is prepared by the PM and must include the strategy that will be followed in assessing overall system vulnerability/lethality in lieu of full-up testing and an assessment of possible alternatives to realistic system testing.

(2) Request for waiver is submitted by the PM to the T&E WIPT for coordination and approval.

(3) For ACAT ID systems:

(a) Upon T&E WIPT approval, the PEO/PM submits the request for waiver through the DUSA (OR) for review and approval by the AAE.

(b) Upon approval by the AAE, the DUSA (OR) submits the request for waiver through the DOT&E for approval and certification to Congress by the Under Secretary of Defense (Acquisition and Technology).

(4) For less than ACAT ID systems, the PEO/PM submits the request for waiver through the DUSA (OR) for approval and certification by the AAE. Certifications and reports outlining the alternative LFT&E strategies will be submitted to Congress through the DOT&E and the Under Secretary of Defense (Acquisition and Technology).

b. The waiver process should normally be considered a last resort in addressing the full-up LFT&E requirement. The development and articulation of a well-planned strategy that takes advantage of extensive component/sub-system/system testing and a limited but reasonable full-up, sub-system/system LFT&E phase can satisfy the LFT&E requirement.

J–26. System evaluation plan

In addition to the evaluation strategy, which defines the evaluation issues, the SEP includes the LFT&E issues and provides the crosswalk between the evaluation issues and the data requirements. Additionally, the data sampling plan and analysis techniques are specified to ensure the logic of the evaluation is understandable. The SEP will identify MOPs and MOEs associated with the issues developed in the strategy. The SEP will include a section describing the types of threats or targets that the system is expected to encounter during the operational life of the system and the key characteristics of the threats/targets that affect system vulnerability/lethality. A reference to the specific threat definition document/authority will be presented with further discussion of the rationale/criteria used to select the specific threats/targets or surrogates and the basis used to determine the number of threats/targets to be tested in the LFT. Any T&E limitations or shortfalls and their impact on the evaluation will be identified. Furthermore, any previous data that will be used to support the evaluation will be discussed. For LFT&E programs, the approved SEP is provided to the DUSA (OR) when the EDP and DTP are submitted for approval (see chap 6). The SEP contains a DSM that identifies the test, existing data, modeling or analyses that will provide the information to address the issues identified in the LFT&E strategy. The SEP also contains the BCM that provides a crosswalk on the user requirements, with specification of the MOP/MOE used to evaluate requirements.

J–27. Event design plan

Subsequent to the development of the SEP, EDPs are developed to detail test conditions and data requirements for use in the development of the DTPs. The EDP also describes statistical analyses, criteria, models, system comparisons, and how they support the evaluation. The EDPs provide the tester or analyst with the details on what data are required from a particular test or analysis event. The EDP will detail the decision process for foreseeable changes in the test design. If an unexpected change in the test design is required, the change to the EDP will be fully coordinated and approved by the DUSA (OR) and DOT&E. For FUSL LFT&E, the EDP is submitted to DUSA (OR) for approval 180 days prior to test initiation and it is subsequently forwarded to DOT&E for approval.

J–28. Pre-shot prediction report

The pre-shot prediction report provides the vulnerability/lethality analysts' best estimate of the expected outcome of each shot before actual test conduct (that is, a pre-shot prediction). It is a requirement for all LFTs and provides a snapshot of the vulnerability/lethality analysts' current understanding of the munition/target interaction.

J–29. System evaluation report

The SER documents the live fire vulnerability/lethality evaluation and contains the assessment of the critical issues and conclusions concerning the vulnerability/lethality and BDAR (vulnerability LF programs only) of the system. The SER addresses the test objectives, issues, and criteria as defined in the SEP, EDPs, and BDAR support plan. It discusses the crosswalk between results and the evaluation and specifies any limitations relative to the analysis. The SER objectively addresses all aspects of the system vulnerability/lethality, both negative and positive. The evaluation will be balanced by the discussion of vulnerability/lethality based on the likelihood of occurrence on the battlefield. Not all vulnerabilities identified in a vulnerability LFT&E can be fixed. Constraints on system funding, system weight, and other aspects necessitate the ranking of the identified vulnerabilities from the perspectives of likelihood of occurrence on the battlefield and the degree of system degradation given an occurrence. The final SER provides this information to the user and to the PM for resolution. The SER is submitted to the DUSA (OR) for review and together with the final test report is forwarded to DOT&E within 120 days after test completion. The SER and all LFT&E reports (to include the OSD assessment report to Congress) must be rendered prior to the FRP decision.

J–30. Model comparison report

The model comparison report includes an in-depth comparison of the pre-shot predictions of crew and system damage and the observed test outcomes. This process requires a detailed examination of component damage states, failure modes, damage mechanisms, and so forth, to ensure a full understanding of model predictive capability.

J–31. Modeling support

Vulnerability/Lethality model outputs, typically generated by, or under the auspices of SLAD for Army programs, are used by AEC along with LF test results to address critical evaluation issues pertaining to system vulnerability or lethality, crew casualties, and logistic supportability. For MDA, the modeling agency is the SMDC. For JLF programs, and Army LFT of multi-Service equipment or munitions, vulnerability/lethality modeling may be conducted or supported by the Navy or Air Force. It is difficult to separate vulnerability and/or lethality evaluations directly supporting FUSL LFT from those required for the entire acquisition process. In a broader context, model-generated vulnerability

and lethality estimates are critical inputs to system effectiveness studies, such as AoAs, designed to determine force exchange ratios, optimum tactical deployment schemes, wartime maintenance and medical requirements, and other measures of system cost and benefit. Thus, there is clearly a critical link between vulnerability/lethality modeling and system level evaluations. The following discussion attempts to provide a better understanding of the Army's vulnerability/lethality models and their role in LFT&E.

a. Much of the early controversy surrounding LFT&E focused on the adequacy of Army vulnerability/lethality models and their appropriate role in the overall LFT&E process. Too often people interpreted the debate over these issues in such a manner that modeling and testing were viewed as an either-or proposition. The fact is both are needed and are essential to a comprehensive and effective LFT&E program. They are complementary efforts and the LFT&E strategy and planning must be based on this view. This guidance attempts to provide a better understanding of the Army's vulnerability/lethality models and their role in LFT&E. Live fire testing, even when supplemented with DT, cannot produce enough data to assess the vulnerability or lethality of a system for all combinations of threat, impact, and engagement conditions. Thus, modeling must be used to extend test results to account for conditions impractical or impossible to test. The reader is reminded that modeling here is defined in the broad sense given in the glossary.

b. In general, more than one model or sub-model must be used to characterize such phenomena as target geometry, munition performance, armor performance, Behind Armor Debris (BAD), personnel injuries, component and subsystem failure modes, aircraft airspeed and altitude dependence, and component kill probabilities. Usually, these models are implemented and applied with personal and mainframe computer codes that, depending on their complexity and sophistication, have modules to implement these models or use as input the products of auxiliary codes. It is important to recognize that the choice of models cannot be specified arbitrarily. Rather, the appropriate model or assessment technique must be chosen on the basis of how much is known about the threat munition or target, input data that are available, and perhaps most importantly, the vulnerability or lethality issues that the LFT&E program is designed to address. While the most detailed and sophisticated models consistent with these criteria should always be used, it is not unusual for one suite of models to be most appropriate for FUSL pre-shot predictions while another suite of models is best for some other aspect of the LFT&E effort. This flexibility in model selection is especially necessary for lethality LFT&E because the level of knowledge of the threat target is often extremely limited.

c. For any given LFT, whether vulnerability or lethality, the suite of analysis models must be selected by the vulnerability/lethality analyst in coordination with the system evaluator. However, once the modeling strategy is determined, it is important to create an audit trail. The underlying rationale for the model or its modification, model limitations, assessment procedures, and required input data should be documented. The models to be used must, of course, be specified in the SEP and appropriate EDPs. However, depending on the level of development of the LFT&E strategy, they may, or may not, be identified in the earliest versions of the TEMP.

d. In the context of LFT&E, vulnerability/lethality modeling has four basic roles in addition to the evaluation support mentioned above. The additional roles include support test designs, guide and evaluate vulnerability reduction or lethality, and methodology diagnosis.

(1) Test design support. To most efficiently utilize resources allocated for the FUSL live fire test, modeling is used as follows:

(a) To determine which engineering shots make the most sense in terms of what is known about the vulnerability or lethality of the system being tested, the expected performance of the threat munitions or target, and the specific evaluation issues for the system being tested.

(b) To develop and apply exclusion rules for randomly selected shots and, once those shots have been selected, to determine from pre-shot predictions that, if any, should be conceded to avoid unnecessary loss of test assets.

(c) To "filter" random or engineering shotlines to ensure a specified level of damage will be considered (for example, using loss of function matrices to identify weapon/target impact locations that satisfy a pre-selected criteria that only "shotlines with a loss of function greater than or less than a certain value will be considered" or to identify weapon or target impact locations that satisfy pre-selected damage criteria).

(d) To assist in shot prioritization from least to most damaging. This will ensure that most of the testing will be completed before the high-risk shots are fired. This works well for both vulnerability and lethality tests since target repair is a major driver in the turnaround time between LFT shots.

(2) Vulnerability reduction/lethality enhancement. Modeling also supports vulnerability reduction and lethality enhancement efforts by allowing the analyst to evaluate the potential payoff of design changes intended to reduce casualties/system vulnerability or increase munition lethality.

(3) Methodology diagnosis. One objective of LFT is to determine the extent to which the vulnerability and lethality models account for all pertinent munition damage mechanisms and target failure modes. In this context, modeling, via comparing pre-shot predictions with test results, can provide insights into the fidelity of the models themselves. Seldom will enough data be generated from a single LFT program to allow a complete verification of model performance,

but insights can be gained to suggest whether significant munition or target interactions are being neglected by the models and to identify areas of model performance that need to be more thoroughly examined in on-going model improvement programs. Note that pre-shot predictions have been mandatory for FUSL LFT programs or the highest fidelity tests conducted as part of a LFT&E strategy. Pre-shot predictions are not required for efforts that are experimental in nature and are conducted to develop model inputs and algorithms. Pre-shot predictions for tests that are neither FUSL nor experimental, may or may not be required. The need for modeling pre-shot predictions should be determined in these cases by the need to validate modeling prior to FUSL or to substantiate that the model adequately predicts the target-threat interaction.

(4) Pre-shot predictions. Pre-shot predictions can be as simple as using a series of charts to determine if missile fragments are likely to sever a drive shaft in the FUSL LFT, or in component or sub-system level tests. At the other extreme, modeling may involve the use of several large-scale computer codes to generate distributions of damaged components or other metrics, which take into account all known munition/target interaction phenomena and, in addition, address the stochastic nature of these interactions.

J–32. Modeling requirements and classes

Early in the system acquisition cycle there is little or no test data, and evaluations are made based upon model estimates and/or analyses. Databases to support the models should reflect the technical and performance characteristics of the system and the threat. The initial models and model inputs will probably be both unrefined and uncertain. The LFT&E strategy should be designed to increase the level of refinement and to reduce the uncertainty. A carefully crafted strategy will make use of early engineering data to refine models and develop a resource efficient building block test program to acquire the necessary data.

a. Regardless of the specific models selected to support any given LFT, there are several databases that must be developed prior to LFT. The exact nature of these databases will, of course, vary depending on the models used. However, they will usually include such things as target descriptions, threat munition and armor performance, BAD characteristics, failure modes and component/sub-system criticality, kill criteria, damage assessment lists, helicopter altitude-airspeed diagrams, and the sensitivity of combustibles to fragment and penetrator impacts. Development of these supporting databases must begin 1 to 2 years in advance of the start of the FUSL LFT. A potential problem with the scheduling of tests and analyses to generate these databases is that the data must be pertinent to the planned production design of the system or munition being tested. For example, penetration characteristics for a new projectile must be for the production design as opposed to evolutionary development prototypes. Some of these databases will be developed wholly or in part to support the overall T&E process; others are needed to directly support FUSL LFT. In any event, costs and hardware requirements must be identified as early as possible in the TEMP in order to permit their inclusion in budget and contractual documents.

b. Also, engineering models may be used to establish the performance of a particular area of the system being evaluated, either vulnerability or lethality. A well-designed strategy will make use of the building-block approach to help refine and validate engineering performance models in the execution of the LFT&E strategy. This approach can be used to build confidences in the engineering models. Some examples are finite element models to determine the blast loading on aircraft structural members, shaped charge jet penetration models, hydracode finite element modeling, shock and blast codes, and many other engineering based models. Care must be used in the selection of the models to be used and the system evaluator will need to understand where the models apply and the limitations of the models (that is, where the models are not intended to provide applicable output to the assessment of the system's performance).

c. The types of models used to support pre-shot predictions for the FUSL LFTs can include engineering models, stochastic V/L models, and simple engineering judgments. Table J–4 compares these classes for output, level of detail and applications.

Table J–4
Comparison of pre-shot modeling capabilities

Model type	Output measures	Level of detail	Applications
Engineering judgment	Expert judgments on the potential for system, sub-system, and component level damage	Judgments can be provided at the component level in terms of a "likely" or most probable outcome	Incorporation of effects from damage mechanisms not addressed by available models
Engineering	Finite Element Models (Hydracodes, Dytan, NASTRAN,	Structural Components and Blast Loading Shaped	Design of Structures and Failure Limits Design of

Table J–4
Comparison of pre-shot modeling capabilities—Continued

	Dyna 3D) Empirical Estimates of Penetration and Behind Armor Debris	Charge Warhead Penetration, BAD Predictions	Warheads
Stochastic Point Burst (for example, MUVES–S2, Advanced Joint Effectiveness Model)	M–Kill Pdf F–Kill Pdf M/F–Kill Pdf K–Kill Pdf Component damage state Pdf	Same as above	Same as above plus estimation of errors in field sampling, propagation of uncertainties, and calibration of lower-level models.

Notes:
* **MUVES** = Modular Unix-based Vulnerability Estimation Suite; **Pdf** = Probability Density Function; **F-Kill** = Firepower Kill; **K-Kill** = Catastrophic Kill; **M-Kill** = Mobility Kill; **M/F Kill** = Mobility or Firepower Kill

d. The vulnerability and lethality estimates do not account for combat attack distributions, deployment conditions, or weapon hit probabilities. Typically, the system evaluator applies these factors to the vulnerability and lethality estimates. Resulting metrics are then used by ATEC, TRADOC, or other agencies to evaluate system survivability or firepower to determine force exchange ratios, identify maintenance requirements, or determine some other measure of system effectiveness. Evaluation strategies must be based on the type, quality, and quantity of vulnerability/lethality estimates that are reasonably expected to be generated in light of the limitations discussed above. In addition, data requirements must be identified in a timely manner to allow input databases to be developed and necessary model modifications to be made.

J–33. Required documentation

a. Pre-shot prediction report. The pre-shot prediction report provides the vulnerability/lethality analysts' best estimate of the expected outcome of each shot before actual test conduct (that is, a pre-shot prediction). It is a requirement for all FUSL LFTs (or substitute test series) and provides a snapshot of the vulnerability/lethality analysts' current understanding of the munition/target interaction. These predictions can range from subjective engineering judgments of the expected damage level through computer-generated estimates of crew casualties and loss of critical system capabilities. The SLAD (or SMDC for MDA programs) is responsible for generating the pre-shot predictions for each FUSL LFT. Appropriate pre-shot prediction techniques will be determined by SLAD/SMDC on a case-by-case basis in conjunction with the system evaluator. The SLAD/SMDC will prepare the pre-shot prediction report. It must be submitted to the DUSA (OR) along with the DTP (60 days before test initiation for FUSL LFTs). The Army approved Pre-shot prediction report is forwarded along with the DTP and the EDP to DOT&E for review and comment.

b. Model comparison report. The model comparison report includes an in-depth comparison of the FUSL LFT pre-shot predictions of crew and system damage and the observed test outcomes. Thus, this report can contain damage assessment information that will be published in the detailed test report as well as additional data analysis. This process requires a detailed examination of component damage states, failure modes, damage mechanisms, and so forth, to ensure a full understanding of model predictive capability. Anomalies will be identified and, if required, model updates specified. Within 6 months after completion of the test, the SLAD/SMDC will publish the model comparison report.

J–34. Verification, validation, and accreditation

See "DA Guidelines: Use of Modeling and Simulation to Support Test and Evaluation," 18 April 2000. With the use of models in system evaluations, there is a requirement to understand the limitations associated with the models used to support system evaluation. The VV&A can be carefully built into a LFT&E strategy in order to provide a method to examine model predictions at various stages of development of the system. Only those portions of the model not previously validated need to be addressed in this stepwise comparison to the test data to ensure the models adequately represent the physics and outcomes that the model is being used to analyze. For applications of the models used in areas previously validated, further validation is not essential. Accreditation is required for models used in support of system evaluations, regardless of previous use, to ensure the models are being used in appropriate fashion. The agency using the model accredits the model for use in the system evaluation with the support of the agency that developed the model.

Appendix K

Reliability, Availability, and Maintainability Issues: System Evaluation Considerations

K–1. Overview of reliability, availability, and maintainability

RAM are important considerations in the acquisition of all systems. The degree of RAM evaluation required can vary widely from one system to another, depending on such factors as system complexity and technological maturity. This appendix defines the RAM related activities of T&E throughout the life cycle of a system. This guidance should be tailored for each program based on the level of complexity of the system, the acquisition phase, acquisition strategy, and the impact of RAM on the performance and suitability of the system. As presented, it illustrates comprehensive application to the most complex systems but is intended for selective application as appropriate.

a. Within the area of suitability, RAM is an important consideration in the acquisition of virtually all systems. RAM has a direct bearing on mission success, as well as on logistical considerations such as maintenance workload, sparing, level of repair decisions, training, and other operating and support cost factors.

b. The system evaluator, in coordination with other members of the T&E WIPT, is responsible for determining the extent and nature of RAM data required for the RAM portion of the system evaluation.

K–2. Reliability, availability, and maintainability definitions

a. Reliability is the duration or probability that a system can perform a specified mission for a specified time in a specified environment. Mission reliability is the reliability associated with completion of a specific MP. It addresses essential function failures that cause either loss of a mission essential function or degradation in performance below ORD requirement levels. It is noted that failures to meet performance requirements can also be caused by other factors, such as design shortcomings, and failure to achieve a performance requirement is not treated as a reliability problem unless it is the result of a reliability incident.

b. Maintainability is a measure of the ability of an item to be retained in, or restored to, a specified condition when maintenance is performed by personnel having specified skill levels and using prescribed procedures and resources, at each prescribed level of maintenance and repair. It reflects the ease and efficiency of performing both corrective and scheduled maintenance on a system.

c. Availability is the probability that a piece of equipment is in an operable and committable state at a given (random) point in time. Repair, maintenance, and administrative and logistics downtime are the most common causes of equipment non-availability for use. A system's availability is a function of its reliability and maintainability.

K–3. Reliability, availability, and maintainability requirements

The CBTDEV or TNGDEV develops the ORD RAM requirements. The ORD RAM requirements provide the CBTDEV's best estimate of what is required to meet the users' effectiveness, suitability, and survivability needs but should also reflect what the MATDEV deems affordable and technically achievable within program funding, risk, and time constraints. The requirements are developed in coordination with the system evaluator through the ICT process. Three elements are required to define RAM requirements—

a. The parameters and their numerical values. The development of a reliability parameter usually assumes that the failure rate of the mature system will be constant over a long period. This assumption allows the requirement to be expressed, not as a probability, but as an easily measurable parameter directly related to reliability. In T&E, the mission reliability parameter is normally one of the following:

(1) Mean time between essential function failures.

(2) Mean time between mission aborts.

b. If the system has another measure of usage other than time, the parameter is expressed with those units, such as miles, rounds, or events between failures. For single shot devices, such as a missile system, reliability is expressed as a ratio of number of successes to number of total attempts.

c. The OMS/MP describes the individual missions that the system is required to perform and the conditions (climate, terrain, and battlefield environment.) under which the missions are to be performed.

(1) The OMS is a description of the anticipated mix of ways the system will be used in performing its operational role. It includes the expected percentage of use in each role and the percentage of time it will be exposed to each type of environmental condition.

(2) The MP is a time-phased description of the operational events and environments an item will experience from beginning to end of a specified mission (including the criteria for mission success or critical failures). The MP is used as the basis for the mission reliability requirement. The MP can be multifunctional (for example, a tank shooting,

moving, and communicating), single-function continuous (that is, continuously performing one task), single-function cycle (that is, repeatedly performing the same task), or single-function one-time.

d. The Failure Definition and Scoring Criteria (FD/SC) are a set of rules designed to provide consistency in the interpretation (such as scoring) of reliability test incidents. The FD/SC define the required functionality and allowable levels of degradation (what constitutes a failure) and establishes a framework for classifying and charging test incidents. The FD/SC is a living document that may evolve as the program progresses and the system configuration and operation evolve.

K–4. Developmental and operational reliability, availability, and maintainability

Both the developmental and operational aspects of RAM are important considerations throughout system development and fielding. A system that meets hardware/software developmental test requirements when tested individually in a controlled environment may not meet mission requirements in an operational environment where it must interact with Soldiers and other systems.

a. Data from DT are required to ensure RAM maturity of the hardware/software prior to entering an operational test. Developmental RAM examines the RAM characteristics based only on the hardware and embedded software of the system. It focuses on the extent to which the system meets technical RAM specifications and reflects those failures for which the system contractor is accountable.

b. Operational RAM considerations for a system relate to its hardware, embedded software, typical operators and maintainers, manuals, tools, TMDE, support equipment, and the operational, organizational, and logistical support concepts. Operational RAM quantifies the degree to which the user can rely on required system functions and the burden associated with keeping those functions at their disposal. The operational RAM assessment cannot be disassociated from the operational scenarios in which the system must function or from the support environment on which the system must rely.

K–5. Reliability, availability, and maintainability management

The management of a RAM program is primarily the responsibility of the MATDEV, who is responsible for establishing and overseeing contracts that result in reliable and maintainable systems. The MATDEV should assess the potential impact of RAM on operations and support cost and the comparative risk associated with the various alternative concepts to achieve RAM requirements. Reliability Centered Maintenance (RCM) techniques are recommended to coordinate maintainability design efforts with maintenance planning. Acquisition and program planning should include early investment in RAM engineering tasks to avoid later cost and/or schedule delays.

a. RAM planning should encompass RAM program requirements, program tasks, reliability growth expectations, contract provisions, test plans, and resources necessary to support these plans. The MATDEV should keep the status of RAM development visible throughout the program and should plan for contractor reviews; data collection; failure reporting, analysis, and corrective actions; failure review boards; and testing and feedback mechanisms, as necessary, to provide insight into design, development and supportability progress, surveillance, and control.

b. Technical reliability thresholds and objectives derived from the operational requirements normally reflect only the hardware and software associated with the contractor-furnished equipment and Government-furnished equipment. The threshold can be used as the minimum acceptable reliability value in the contract. Before contracts are finalized, the MATDEV should coordinate contract RAM requirements with the CBTDEV, matrix support elements, and system evaluators. Both technical and operational RAM requirements are to be demonstrated with high statistical confidence. High confidence is usually considered to be the 80 percent level; however, tailoring based on test cost or mission criticality is encouraged and the chosen confidence/risk value should be reflected in the TEMP.

c. Solicitations and contracts should provide adequate visibility into system development to assure that systems are designed to meet RAM requirements, that RAM performance can be effectively tested, and that compliance with requirements can be evaluated.

d. The MATDEV ensures appropriate consideration is given to the following factors in program planning:

(1) Failure modes, effects, and criticality analysis.

(2) A test, analyze, and fix process.

(3) Use of RAM conferences to independently assess and monitor the growth process.

(4) System level testing to confirm achievement of interim and final RAM requirements.

(5) A closed loop, Failure Reporting/Analysis and Corrective Action System.

(6) Accelerated growth testing—testing at stress conditions higher than normal to precipitate failures at a faster rate.

(7) Engineering failure mechanism analyses (such as physics-of-failure analyses).

e. Reliability growth methodology, MIL–HDBK–189, provides an effective tool for planning and evaluating system reliability and an effective baseline against which actual growth can be managed. The MATDEV should apply reliability growth management methodology on all programs at the system level and, whenever practical, at the subsystem and major component level.

f. The MATDEV continuously assesses the performance of developed and fielded systems to identify opportunities for system RAM improvements, either through capability enhancement or through support burden and operations and support cost reduction.

g. Throughout the materiel life cycle, the MATDEV maintains a historical audit trail of RAM development that includes but is not limited to—

(1) RAM requirements, to include the failure definitions and scoring criteria and OMS/MP.

(2) RAM planning documentation, current and historical growth curves, and contractual RAM provisions.

(3) Test data (to include type of test, system configuration, test conditions, test length, failures, data analysis, problems, root-cause failure analysis, and corrective actions).

(4) RAM status at key points in development, production and field operation.

(5) RAM improvements.

K–6. Evaluation planning

Evaluation planning is oriented toward providing data with which to estimate the technical and operational RAM values expressed in the requirements document. Tests are designed to ensure that statistically adequate estimates of RAM values are provided. The system evaluator is responsible for analyzing system RAM characteristics and evaluating RAM characteristics and performance. This requires selective participation in acquisition events, input to select planning documents, and development of a plan to quantify system RAM characteristics in terms of mission objectives. This plan requires the system evaluator's understanding of and input to the definitions of the operating and support environments, the operational tasks required of the system, acceptable levels of task performance, and the relationship of tasks to mission objectives.

a. The SEP reflects the system evaluators and testers' plan for the T&E of system RAM and its relation to the technical requirements and the operational effectiveness and suitability of the system. The RAM technical characteristics and the RAM critical and additional operational issues provide the vehicle for translating the RAM related requirements into criteria, MOPs, and data requirements in planning.

b. Coordination within the T&E WIPT must occur early in the planning process to ensure that RAM requirements and RAM data collection systems are adequately defined and to allow adequate time to set up RAM software programs, develop data collection plans, and conduct training prior to the pilot test.

K–7. Reliability, availability, and maintainability subgroup of the test and evaluation working-level integrated product team

The RAM Subgroup of the T&E WIPT reviews, classifies (that is, the RAM Scoring Conference scoring of test incidents), and charges (that is, assignment of causality) RAM data from system level tests. All data from system level RAM testing that record degradation from anticipated system performance should be scored in accordance with FD/SC. See DA Pam 70–3 for detailed guidance.

a. The RAM WIPT is made up of representatives from the MATDEV, CBTDEV, TNGDEV, and the independent system evaluator and may be augmented by others as appropriate. The testers should attend in an advisory capacity. Official scoring (that is, classification and chargeability) is the responsibility of the MATDEV, CBTDEV (or TNGDEV), and the system evaluator.

b. The TEMP is annotated to reflect those tests for which the system evaluator will serve as chair for RAM Scoring Conferences. The MATDEV chairs all other RAM groups. Prior to the first meeting, the chair coordinates with the participating organizations to establish membership, establish a common understanding of the system requirements, and identify a single voting member from each organization.

c. RAM WIPTs should meet periodically during system level testing, and a final meeting should be held at the conclusion of each test.

K–8. Reliability, availability, and maintainability assessment conference

The purpose of the RAM assessment conference is to establish a final RAM database from which assessment of operational and technical RAM requirements and specifications will be made. The assessment conference determines the viability of aggregating individual test databases and determines the impact of validating corrective action on that data. See DA Pam 70–3 for detailed guidance.

a. The system evaluator is responsible for chairing the RAM assessment conference. Membership is the same as the RAM scoring conference.

b. A RAM assessment is usually held at the completion of an acquisition phase or before a program decision.

K–9. Contractor participation in reliability, availability, and maintainability scoring and assessment conferences

By law, system contractor personnel will not attend or be directly involved as members or observers in RAM scoring or assessment conferences that address data intended to support evaluation of the system's operational RAM parameters.

a. Discussions with system contractor personnel are held separately from scoring and assessment activities. If the MATDEV needs access to contractor expertise during the conference, the chair may, at their discretion, recess the meeting to permit consultation with the contractor. The chair may, subject to the dissent of any spokesperson, allow the MATDEV to provide a contractor technical presentation on a pertinent aspect of the system to the members during the recess. Conference members may question the contractor representatives regarding the incident but may not discuss any proposed scoring with the contractor present. The scoring or assessment conference chair maintains a written record of the nature of the contractor/Government discussions.

b. This restriction applies to the scoring of DT data if the results may be used to support the evaluation of the system's operational RAM parameters.

K–10. Corrective action process

This process begins at the RAM Scoring Conference or in cases of critical incidents at the time of the incident.

a. As part of the evaluation of test events, the RAM Scoring Conference designates responsibility for investigating the incident, initiating corrective action, and reporting the results. Activities responsible for corrective action include the MATDEV for hardware, software, TMDE, manuals, and support equipment; the tester for failures caused by improper test conditions; and the CBTDEV for failures related to training and operational concepts. Each activity initiates appropriate corrective actions and provides a detailed analysis of these incidents to the members of the RAM Assessment Conference. The MATDEV takes the lead in the analysis of failure incidents, and sponsors corrective action reviews as appropriate. The status of corrective actions will be provided to the RAM Assessment Conference members.

b. After the test, the MATDEV may call a corrective action review team (CART) meeting. The CART process is a tool that supports the MATDEV's required corrective action review process. Its purpose is to determine adequacy and effectiveness of planned and implemented corrective actions. The CART is usually composed of the same members as the RAM Assessment Conference. In developing estimates of projected system RAM characteristics, results of the CART are considered. These estimates or projections may be included in the system evaluation and compared to the system's RAM requirements.

K–11. Use of reliability growth/projection methodologies in the test and evaluation process

Reliability growth methodologies will be used, where appropriate, to assess program progress toward meeting developmental and operational reliability requirement parameters and thresholds. Growth methodology application may be useful in the event that OT reliability results are not demonstrated with confidence due to test duration limitations. Given compatibility with respect to test environments (and model fit), the growth tracking curve may be extended to include the OT data point (estimate) resulting in a new estimate based on augmented data. Projection methodologies can be used as risk mitigation tools in ascertaining readiness to enter the next test phase based on the previous completed test phase and identified delayed fixes. Projections are never to be utilized as a means to "demonstrate" reliability requirements. In addition, projection methodologies may be used in RAM Assessment Conferences for determining a projected reliability (based on a fix effectiveness assessment) when the reliability estimate (based on test results) falls below the requirement or threshold at a milestone decision point. This can provide useful information regarding risk relative to reliability achievement and whether to enter the next acquisition phase. Unique application of growth or projection methodologies may require support from AMSAA.

Appendix L

Logistics Supportability (Including Transportability) Issue: System Evaluation Considerations

L–1. Overview of logistics supportability

a. Army policy requires supportability to be co-equal in importance with cost, schedule, and performance to ensure that supportability issues are addressed early and throughout the life cycle of the system. Therefore, the Army's ILS program is an inherent part of the development and fielding of a system. It provides for all the necessary support resources to ensure the supportability and readiness of the system when fielded. The system evaluator works closely with the Army logistician and the acquisition community through the IPT process to provide a continuous assessment of the logistics support of a program and associated software.

b. The Army logistician (HQDA, ASA (ALT) ILS) facilitates the development and integration of the ILS elements (see AR 700–127) for all assigned acquisition programs. The logistician participates in developing requirements, supportability strategies, and fielding plans; participates in the system IPTs, the T&E WIPT, and signs the TEMP as the Army logistician; and participates in DRs.

c. The MATDEV provides an ILS manager who will be the focal point for all ILS actions for the program and who chairs the supportability integrated product team (SIPT).

d. The system evaluator is a member of the SIPT and provides a continuous assessment of the system to ensure that readiness and supportability objectives are identified and achieved. The evaluation strategy will—

(1) Ensure the ILS assessment considers compatibility with the testing strategy.

(2) Identify, track, and report logistics supportability deficiencies and shortcomings.

(3) Provide for testing of the system's logistics support concepts, doctrine, organization, and hardware and ancillary materiel in the intended environment.

(4) Provide CE of the system throughout its life cycle and provide data as required.

L–2. Supportability Integrated Product Team

The SIPT is a working-level IPT, chaired by the ILS manager. It provides support to the ILS manager in the requirements generation, development, and acquisition process for ILS elements. Its members include the CBTDEV, MATDEV, Corps of Engineers, Army logistician, testers, transportation representative, and system evaluator. Membership is based on the scope of the program and may be expanded as necessary. The SIPT is a working body, and the roles and responsibilities of its members will be prescribed in the Supportability Strategy. It works with other bodies (such as the T&E WIPT) to ensure an integrated effort.

L–3. Supportability strategy

The ILS manager is responsible for developing a Supportability Strategy that defines the complete ILS strategy for a system. Supportability is a critical factor of suitability in evaluating test objectives, issues, and criteria, as well as in the source selection evaluation. The initial Supportability Strategy is coordinated with the CBTDEV, MATDEV, logistician, testers and evaluators. It will be available 60 days prior to MS A and is updated at DRs and at other points when required.

a. The approved Supportability Strategy, together with the SIPT minutes, provides an action guide for all ILS program participants. It is used for assigning action items and scheduling completion dates as well as for prescribing system acquisition events and processes requiring ILS action, interface, or support requirements. Included in the Supportability Strategy is identification of the specific ILS test issues related to the individual ILS elements and the overall system support and readiness objectives.

b. A complete set of ILS issues and criteria is included in the TEMP. It is of critical importance that all test resources required for ILS testing be identified in the TEMP to ensure that appropriate resources are budgeted and allocated for testing.

L–4. Integrated logistics support evaluation planning

The evaluation strategy in the SEP will identify, track, and report ILS deficiencies and shortcomings; ensure data availability for the system's logistics support concepts, doctrine, organization, and hardware and ancillary materiel in the intended environment; and provide CE throughout the life cycle of the program.

a. The strategy is developed early in the acquisition cycle, and includes determining when a LD will be performed, if needed. A level-of-repair analysis should be accomplished early in the life cycle to guide test planning for supportability issues.

b. Subsequent testing, M&S, and field experience will be used to improve the matured logistics support program; to determine the effectiveness, adequacy, performance, and reliability and maintainability of system-peculiar support equipment, test program sets, support software, and TMDE; and to update the system repair parts provisioning documentation. In addition to the logistic demonstration, logistics supportability testing includes all testing conducted during the design and development of the system that provides data on supportability issues.

c. The system evaluators, in coordination with the testers, will ensure that a full range of supportability characteristics and issues are developed and that tests are designed specifically to address these characteristics and issues. All data collected during the conduct of the test program will be utilized to reduce the dedicated ILS testing and ensure maximum efficiency.

d. The emphasis of the ILS evaluation changes as the program moves through the acquisition phases. During early phases of a program, the evaluation results are used primarily to verify analysis and develop future projections. As the program moves into Engineering and Manufacturing Development and hardware becomes available, the evaluation addresses design, particularly the reliability and maintainability aspects, training programs, support equipment adequacy, personnel skills and availability, and technical publications. After the FRP decision, the system evaluation provides an update of the status of supportability issues for the materiel release process.

L–5. Logistic demonstration

The SIPT develops a logistic demonstration plan based on the outcome of the review of the requirements and the initial analyses. The plan incorporates all opportunities for data sources to confirm adequacy of the planned support. Support resources are programmed to include use of existing data from the contractor or other users, TM validation and verification, maintainability and BIT demonstrations, transportability analysis, MANPRINT assessments, TMDE assessments, and software assessments. Normally, the logistic demonstration is completed 6 months prior to scored testing in order to correct identified problems. See paragraph 6–23*a*(7) of this pamphlet, AR 700–127, and DA Pam 700–127 for a further discussion of the logistic demonstration.

L–6. System support package

The SSP is a composite of the support resources that will be evaluated during testing. It consists of spare and repair parts, manuals, training package, special tools and TMDE, and unique software. The SSP, used to validate the support system, is to be differentiated from other logistic support resources and services required for initiating the test and maintaining test continuity. The SSP is flexible and is tailored to the system-peculiar requirements and related to supportability testing issues. The SSPCL is provided 60 days before testing begins. The SSP is delivered to the test site not later than 30 days before testing is scheduled to begin. Delays in the availability of certain support items could prevent the test from proceeding on schedule or could result in the test proceeding without conducting the complete evaluation of the support system. This could be costly due to on-site support personnel on hold or tightly scheduled system ranges and expensive test resources not being properly utilized.

L–7. Integrated logistical support evaluation issues

The 10 elements of ILS are defined in AR 700–127 and DA Pam 700–127. The ILS issues and objectives for each element are addressed in the Supportability Strategy and incorporated into the TEMP, including plans for the Logistic Demonstration. Not all ILS elements will be evaluated for all systems, but consideration will be given to each in the Supportability Strategy. For each testable resource in the SSP, a logistics burden analysis is planned for in the SEP and evaluated in the SER. The logistics burden analysis compares support maintenance, supply, and transportation demands placed on the support system against the resources planned for the support system. The SSP is to be addressed to determine the strengths and weaknesses of the planned support in terms meaningful to the decision process.

a. Maintenance planning—The maintenance concept, including all levels of maintenance, tradeoffs, and tasks required to sustain the item at the defined level of readiness, is addressed. Operational readiness issues address the capability and capacity of the unit to achieve and maintain the required peacetime and wartime system readiness objectives (SROs) when the planned logistics support concepts, doctrine, and organization and materiel are used.

(1) The issue is normally limited to the retail (intermediate and below) Army logistics system. In cases where two levels of logistics support are dictated, such as user and depot, the operational readiness issue will include the depot activity. Criteria normally come from the SRO in the ORD.

(2) The SEP shows how the SRO will be estimated, how unit readiness will be assessed, and how significant drivers for the SRO will be determined.

b. MANPRINT and personnel—Maintenance, operation, and other support personnel and their required skills and training are the considerations for this element. See appendix M for details.

c. Supply support is divided into the following categories:

(1) Mission-critical support (that is, supply support necessary to sustain the system in combat).
(2) Non-mission-critical support.
(3) Items common to the unit's existing supply support.
(4) System-peculiar items introduced into the unit's existing supply support. The evaluation strategy will consider the following: demand, consumption rates, mobility, size, and capacity.

d. Equipment support (see AR 750–43) includes all common or general-purpose manual test equipment and automatic test equipment; TMDE; intermediate forward test equipment composed of a contact test set, base station test facility, an electro-optical test facility at the intermediate level; test program sets, BITE, and calibration equipment.

(1) TMDE may be acquired under a separate requirements document or in a separate annex to the supported end item requirements document. In either case, it has its own performance, RAM, and logistics requirements. Formal procedures have been established for justifying and acquiring special-purpose TMDE. Each TMDE requirements document, product improvements, and TMDE annex to the supported end item has a MNS concept. All TMDE will be evaluated to determine that its capabilities during the required LD can be met in the operational environments. Special exercises may be required to include fault insertion events to fully evaluate TMDE capabilities.

(2) BITE is used in fault detection, isolation, or location and involves digital or analog signals, warning and advisory messages, lights, audio signals, or switches. It is usually planned to detect, isolate, or locate a percentage of system faults to a specific ambiguity group level, line replaceable unit (LRU), or shop-replaceable unit (see glossary for definitions). The evaluation examines BITE effectiveness, software, and growth during system development. BITE data requirements are to be included in instrumentation requirements.

e. Technical documentation includes all manuals and any other documents on specific maintenance, special inspections, lubrication, or other instructions. Software documentation is addressed as a separate item because of its criticality. The evaluation of manuals consists of two distinct tasks. The two tasks are accomplished separately, in order to determine if the manual is in error or if the user failed to follow the procedures. The two tasks are—

(1) Determine if the drawings, figures, specifications, and procedures are technically correct. This is usually accomplished during DT and logistic demonstrations.

(2) Determine if the Soldier can understand and correctly perform the procedures. This is accomplished during OT, and includes ensuring that tools, TMDE, support equipment, supply support, and critical tasks are allocated by the manuals to the correct level of maintenance and MOS.

f. Training and training support (AR 350–1) includes training aids, simulators, training materials, instructors, and on-the-job training. It is provided to the testers, controllers, support personnel, data collectors, and data reducers. Data requirements for training are collected under manpower, personnel, and MANPRINT (see app M).

(1) There are two training TSPs: the NET TSP and the training TSP. Milestones for providing training TSPs to the testers and evaluators will be identified in the TEMP. See chapter 6 for a complete discussion of TSPs.

(2) Evaluation of training and training support is necessary to ensure that the skills and knowledge necessary to operate and maintain a system can be attained and sustained within realistic training environments by units using personnel of the type and qualification expected to use the system when deployed. The extent of these evaluations is defined in the SEP and is contingent on the stage of development of the system being tested. Ordinarily, training is contractor-administered in the early phases of system development. For subsequent phases, the MATDEV provides training to military instructor personnel, who then train the test participants. The objective of the evaluation is to assess the adequacy of training associated with fielding the system.

g. Computer resources support (computer hardware and software) issues are addressed in the SEP. Planning for testing and evaluation of PDSS is included. See appendix Q for software considerations.

h. The adequacy of existing facilities (both fixed and mobile) for the system and its maintenance and support needs must be considered as addressed in the Supportability Strategy. If inadequate, modifications or new facilities will be addressed to ensure support system will operate within planned construction.

i. Packaging, handling, storage, and transportation system-unique requirements and constraints for packaging, handling, storage, and transportation of components, parts, and test equipment must be considered. Transportability is a major consideration in the T&E of Army systems, including system components and spare parts.

j. Design interface supportability issues will influence the system design and consequently, the source selection and acquisition decisions. Design constraints related to ILS must be taken into consideration, such as environmental constraints, interoperability requirements, human factors constraints, deployment concepts, and logistics related durability. See appendix M for MANPRINT considerations.

L–8. Transportability issues (see AR 70–47)

Transportability refers to the ability of a system to be moved by towing, self-propulsion, or by carrier via railway, highway, air, waterway, or helicopter, and airdrop modes of transportation utilizing existing or planned transportation

assets. Transportability is a major consideration in the T&E of Army systems, including system components and spare parts. T&E of transportability will address the end-item in its tactical and packaged or shipping configurations, as well as associated support equipment and TMDE. This focus will allow the system evaluator to determine if the system is deployable.

a. DT is conducted to demonstrate the ability of a system to withstand the expected transportation environment over the useful life of the system before the production decision. During OT, Soldiers who prepare the system for movement are used under realistic conditions.

b. The evaluation strategy will address the following:

(1) The ability to carry the load, as well as the availability of the mode of transportation.

(2) Ensure the weight and dimensions of the new system can be supported by the current bridging (including tactical bridging) and transportation network in the required operational environment.

(3) For large systems such as vehicles, the major source of evaluation information for transportability is the Military Traffic Management Command Transportation (MTMC). As the Army's transportability agent, MTMC provides transportability approvals or recommendations for correcting deficiencies on new systems.

(4) Most of the airlift, sealift, and rail transportation requirements are documented in AR 70–47. The system evaluator should ensure that the MTMC or other approved agency conducts a transportability assessment. For smaller systems the analysis may consist of assessing the unit's capability to carry the new system in addition to the required load.

L–9. Other support equipment

Other support equipment includes generators, trucks, trailers, transportation and handling equipment, shop and supply vans, retrieval and re-supply vehicles, calibration vehicles, ammunition and fuel trucks, and bridges. The evaluation of support equipment (both old and new) compares test data against amounts stated in the basis of issue plan.

Appendix M

Manpower and Personnel Integration Issue: System Evaluation Considerations

M–1. Overview of manpower and personnel

MANPRINT is an engineering analysis and management process to identify and articulate requirements and constraints of human resources, human performance, and hazards to personnel to ensure the "human" is fully and continuously considered in the system design. The assessment of MANPRINT is an essential element of a system's evaluation strategy at each decision point. The evaluation focuses on assessing the status of the system by identifying problems and recommending fixes when human performance problems degrade overall system performance. Both system design and operator/maintainer issues can be a source of MANPRINT issues. (See AR 602–2.) The MANPRINT program includes seven domains—

a. Manpower deals with the number of people in the force structure, irrespective of skill level, required to sustain operations under combat conditions and to maintain and support a system.

b. Personnel addresses the ability to provide qualified people for specific skills needed to operate, maintain, and support a system.

c. Training considers time and resources required to develop the correct skill levels.

d. HFE considers the characteristics of people (physical, cultural, mental) that must be addressed in designing a system (known as an ergonomic science, this addresses all aspects of the Soldier-machine interface).

e. System safety considers the safety engineering principles and standards necessary to optimize safety within the bounds of operational effectiveness, time, and cost.

f. Health hazards consider conditions that can cause illness, disability, or reduced job performance.

g. Soldier survivability considers fratricide, killed in action, and wounded in action prevention.

M–2. System Manpower and Personnel Integration Management Plan

The SMMP is a tailored planning and management tool that outlines and documents the MANPRINT management approach, associated decision and planning efforts, user concerns, and resolution of MANPRINT issues. As the primary issue tracking document, the SMMP is the cornerstone of the MANPRINT effort to ensure human considerations are effectively integrated into the development and acquisition of Army systems. It provides the basis for developing testable issues and criteria about human performance. The SMMP provides input to the TEMP and the SEP.

M–3. Manpower and personnel integration considerations in the evaluation strategy

The most productive, cost-effective time to find and fix human performance problems is early in the system design process, when designs or changes to designs that facilitate human and system performance can be made at the least cost.

a. With input from the lead MANPRINT domain agencies (see AR 602–2), and based on a thorough analysis of the SMMP, the system evaluator develops an effective strategy to produce valid, reliable, quantitative and qualitative data early and iteratively, which provides rapid feedback to the MATDEV's system engineering process. It consists of a detailed front-end analysis designed to produce the most cost-effective integration of MANPRINT issues and concerns. This integrated evaluation approach will give the acquisition team a continual focus on the effects of human performance as an integral component of system performance and will leverage all data collection and analysis efforts. The goal is to resolve human performance issues before the IOT.

b. User performance of tasks critical to overall system effectiveness, suitability, and survivability can be measured in terms of the accuracy of performance and time to perform. These data provide the quantitative basis for the MANPRINT evaluation.

c. MANPRINT analysis is best practiced as an iterative, continuous feedback loop to the MATDEV throughout the design process, rather than as a decision-oriented go, no-go assessment of MANPRINT compliance provided by the system evaluator just prior to the milestone decision.

Appendix N

System Safety Issue: System Evaluation Considerations

N–1. Overview of system safety

Army policy requires that system safety be applied and tailored to all Army systems throughout their life cycle and that safety and health verifications/evaluation be an integral part of the system safety effort. One of the most important aspects of testing is verification of the elimination or control of safety and health hazards. DT provides determinations of personnel and equipment hazards inherent in the system and associated operation and maintenance hazards, with special attention given to verifying the adequacy of safety and warning devices and other measures employed to control hazards.

N–2. Safety evaluation

Within ATEC, the developmental testers (DTC) serve as the Army's system safety verifier. In this capacity, DTC provides both the safety release and the safety confirmation.

N–3. Safety release

The safety release is prepared by DTC and provided to the testing organization prior to any testing using Soldiers. See chapter 6 for details.

N–4. Safety confirmation

AR 385–10 requires that a safety confirmation be prepared at the end of each phase of the acquisition process and at major decision points. Headquarters DTC is responsible for providing the safety confirmation for all systems. The safety confirmation is prepared and provided to the system evaluator and is attached to the SER as an appendix. The safety confirmation will also be provided to the PM, the AMC Safety Office, U.S. Army Safety Center, TRADOC Safety Office, and the MATDEV or PM-supporting Safety Office to support system materiel release. The safety confirmation will—

a. Indicate whether the system is completely safe for operation or identify hazards that are not adequately controlled using MIL–STD–882 and AR 385–10 for classification of the hazards.

b. List any technical or operational limitations or precautions.

c. Highlight any safety problems that require further investigation and testing.

N–5. Hazard analysis

a. Hazard analyses are the heart of the system safety evaluation and provide the preparer of the SAR, safety release, and safety confirmation with a wealth of information. The types of analyses that are performed must be stated in section 4, Safety Engineering of the System Assessment Report.

b. From the beginning, a system must be designed to eliminate or control all potential and actual safety and health hazards. These hazards will be identified in accordance with hazard evaluation techniques and these techniques result in the various hazard analysis documents. The following documents reflect hazard evaluation techniques:

(1) The preliminary hazard analysis is an inductive process that should be conducted early in the design phase of the system life cycle to identify in broad terms the potential hazards associated with the proposed operational concept. The preliminary hazard analysis is prepared by the PM or contractor. It reflects the initial risk assessment of a system and identifies safety critical areas, evaluates hazards, and identifies the safety design criteria to be used.

(2) A system hazard analysis (SHA) is submitted by the contractor in accordance with the requirements of the contract data requirements list. It is a systematic assessment of real and potential hazards associated with possible subsystem failure. It identifies hazards and then directs design efforts toward the elimination or control of the hazard. The SHA indicates the hazard severity and the hazard probability levels as established by MIL–STD–882.

(3) The subsystem hazard analysis report is prepared by the PM or contractor. This report identifies hazards associated with component failure modes and functional relationships of components and equipment comprising each subsystem. The subsystem hazard analysis is an inductive process that, in effect, is an expansion of, with increased complexity over, the SHA. It normally occurs during the design phase; however, it can be used during operation as an investigation to establish cause and effect relationships and probabilities.

(4) The operating and support hazard analysis report is prepared by the PM or contractor. This report identifies hazards and determines safety requirements for personnel, procedures, and equipment during production, testing, installation, training, escape, and operations. It, too, provides information that can be used in preparing the safety release and safety confirmation. The operating and support hazard analysis is normally conducted on all identified hazards

involving man/machine interfaces. It helps ensure that corrective or preventive measures will be taken to minimize the possibility that any human error procedure will result in injury or system damage.

c. The preliminary hazard analysis/list is prepared by the PM. It involves making a study during concept or early development of a system to determine the hazards that could be present during operational use.

d. The software hazard analysis should cover the areas reflected at table N–1 as relating to the safety release. ITOP 1–1–056 describes the software testing procedures.

e. The safety release is a formal document issued by DTC to the operational tester or other user before any hands-on training, use, or maintenance by Soldiers. Copies of the safety release are also issued to the system evaluators, CBTDEVs, and PMs. OT, including pretest system training, and DT involving borrowed Soldiers will not begin until the test agency, the trainer, and the commander who is providing the test Soldiers have received a safety release. DTC does not provide the safety release for systems developed by the USAMEDCOM or for those non-tactical C4/IT systems assigned to CECOM by the CIO/G–6 or AMC.

f. The safety release indicates the system is safe for use and maintenance during the specified test by typical user troops and describes the specific hazards of the system based on test results, inspections, and system safety analyses. Operational limits and precautions are also included.

g. The requirement for a safety release also applies to testing of new or innovative procedures (doctrine and tactics) for the use of materiel that has been type classified. Safety releases are not required for use of standard equipment in the normal prescribed manner.

h. A conditional safety release is issued when further safety data are pending or operational restrictions are required and restricts certain aspects of the test (for example, a restriction on range fan area until all range safety tests are completed). A limited safety release is issued on one particular system (prototype, model, modification, and software revision) or for one particular test.

i. The tester uses the information contained in the safety release to integrate safety into test controls and procedures and to determine if the test objectives can be met within these limits.

j. When unusual health hazards exist, The Surgeon General reviews or participates in preparation of safety releases to ensure safety of Soldiers during OT.

k. The safety release is developed at least 60 days prior to pretest training and all types of OT and DT that expose Soldiers to training and testing activities involving the research, development, operation, maintenance, repair, or support of operational and training materiel. This requires that pertinent data (for example, results of safety testing and hazard classification) be provided to the safety release authority in sufficient time to perform this testing or determine if additional testing is required.

l. The safety release format is reflected in AR 385–10.

N–6. Safety requirements

The human systems integration portion of the ORD contains the system safety requirements. The essential features needed must be clearly stated so that the technical parameters provide the necessary data to verify or address system safety. The critical system characteristics should contain a clear requirement for safety parameters.

a. Prior to MS B, the MATDEV charters the system safety WIPT. This group tailors the safety documents to the requirements of the system being developed. This is done through a variety of documents that are sources of information during preparation of the safety release.

(1) *System safety management plan.* Prepared by the MATDEV, the SSMP is a description of planned methods to be used by the Government in monitoring the contractor's system safety program. It should be reviewed to ensure that ATEC is provided an opportunity to review the requirements and program documents; that the milestone schedule identifies the timely issuance of the SA report to DTC; and that DTC is provided the results of contractor testing. It identifies system safety management issues and is incorporated as part of the Acquisition Strategy for all systems.

(2) *System safety program plan.* The MATDEV will ensure that the contractor prepares and updates a system safety program plan (SSPP). The Safety Verification section should be reviewed to determine the adequacy of procedures for feedback of test information for review and analysis, and the adequacy of procedures established by the contractor's safety organization to ensure safe conduct of all tests. This plan is a description of the contractor's methods to implement the tailored requirements of MIL–STD–882, including organizational responsibilities, resources, milestones, depth of effort, and integration with other program engineering and management activities as well as those of related system.

(3) *Health hazard assessment report.* The HHAR is prepared by the CHPPM at the request of the PM for those systems that require medical advice or assistance for the developmental evaluation of health hazards.

(4) *Safety assessment report.* The MATDEV prepares the SAR or obtains it from the contractor, and provides it to DTC. DTC will not accept a SAR as official unless it has been approved by the MATDEV's supporting safety

office. The SAR references the HHAR and includes information on health hazards. It is a formal summary of the safety data collected during the design and development of the system. The MATDEV summarizes the hazard potential of the item, provides a risk assessment, and recommends procedures or other corrective actions to reduce these hazards to an acceptable level. This is a key source of data for the safety release. The SAR is updated when changes are made that impact safety.

(5) *System safety risk assessment.* The SSRA provides a comprehensive evaluation of the safety risk being assumed for the system under consideration at the milestone DR. This document is prepared by the MATDEV and supports the decision for accepting residual hazards.

b. Risk assessment criteria contained in MIL–STD–882 is used to assess risks in Army systems and facilities. Based on these criteria, risks will be categorized in a three-tiered hierarchy that is tailored to the individual system requirements and which is applicable to the individual program decision authority structure. Table N–1 provides the hazard probability categories as reflected in MIL–STD–882.

c. The model for risk acceptance authority is reflected in MIL–STD–882. This model can be used for any program if appropriate. Should program requirements dictate a different decision authority, an appropriate matrix is developed by the MATDEV. The recommended matrix will be submitted for approval (as part of the Acquisition Strategy) to the AAE or designated authority. The risk acceptance hierarchy is to be published and updated as required in the appropriate SSMP.

d. In order to obtain safety related data, testing must be completed that is safety specific (for example, noxious fumes or toxic gases, operation at the boundary of the operating environment, and software overload tests). Safety representatives will provide specific software conditions to test for and to be included in the formal test plans and procedures. Most safety related data are obtained during conduct of performance and endurance tests. Therefore, while safety specific tests can be conducted early in the program to provide information for a safety release, the information reflected in the test report and safety confirmation addresses all testing.

e. MIL–STD–882 provides uniform requirements for developing and implementing a system safety program of sufficient comprehensiveness to identify the hazards of a system and to ensure that adequate measures are taken to eliminate or control the hazards.

f. The safety confirmation is based on data from specific safety and health tests performed on hazardous devices, components, or by-products to determine the nature and extent of hazards presented by the materiel. Particular attention is given to identifying and assessing special safety and health hazards presented by radioactive materials, RF emitters, toxic gases, laser devices, toxic and carcinogenic materials, gaseous emissions, blast overpressure, and harmful noise sources.

Table N–1
Safety verification process—hazard probability categories (MIL–STD–882)—Continued

	Hazard Probability				
	Frequent	Reasonably probable	Occasional	Remote	Improbable
Specific individual item	Likely to occur frequently	Will occur several times in life of the item	Likely to occur sometime in the life of item	Unlikely but possible to occur in the life of item	So unlikely it can be assumed the occurrence may not be experienced
Fleet or inventory	Continuously experienced	Will occur frequently	Will occur several times	Unlikely but can reasonably be expected	Unlikely to occur but possible
Hazard Severity					
Catastrophic I. May cause death or loss of system	High	High	High	High	Medium
Critical II. May cause severe injury, severe occupational illness, or major system damage	High	High	High	Medium	Low
Marginal III. May cause minor injury, minor occupational illness or minor system damage	High	Medium	Medium	Low	Low
Negligible IV. May cause less than minor injury, occupational illness or system damage	Medium	Low	Low	Low	Low

Appendix O

Interoperability Issue: System Evaluation Considerations

O–1. Overview of interoperability

OSD requires that all acquired systems be interoperable with other U.S. and allied systems, as defined in the requirements and interoperability documents. Interoperability issues will be considered in all early operational assessments and the T&E strategy.

a. The TEMP must include at least one CTP and one operational effectiveness issue for the evaluation of interoperability (see chap 3).

b. The system evaluator reviews the major documents that define the system's interoperability environment and monitors the major events that produce information on interoperability as well as compatibility. The following are the potential sources of interoperability information:

(1) ABIC is produced by the CBTDEV, usually TRADOC, and identifies the intra-Army, inter-Service, and NATO systems architecture and associated interfaces. It serves as the primary document that defines the systems with which a developing system is expected to operate.

(2) User interface requirements are the documents developed by the CBTDEV and provide quantifiable data to characterize each required information exchange.

(3) Technical interface design plans are the technical design documents for each interface. They are developed by the MATDEV and provide the technical interface parameters, message formats, message content, and implementation requirements.

(4) Interface specifications are developed by the MATDEV and provide detailed technical engineering information on system interfaces.

(5) Interface control documents, developed by the MATDEV, describe the physical and electrical connections, voltage, and current requirements, and provide interface control drawings.

(6) Joint Interface Operating Procedures, developed by the MATDEV, describe the man-machine interfaces and standardized operating procedures for multiple interfacing systems. For these joint system interfaces, interoperability is guided by the appropriate military standards (MIL–STDs).

(7) For NATO system interfaces, interoperability is guided by STANAGs.

(8) Interface design handbooks are developed in parallel with the system by the MATDEV in coordination with the user, and provide SOPs and user procedures relevant to the operation of the system under development.

(9) IERs, developed by the CBTDEV in coordination with the MATDEV, describe the communications, data, and message exchange requirements as well as standardized procedures for multiple interoperating systems.

c. The ORD and ABIC enable the system evaluator to identify the interfacing systems and the systems for which interface is a concern. The ORD and user interface requirements are used to identify the factors and conditions that have the potential to impact the system's interoperability requirements. Compatibility issues are identified by the system evaluator based on review of the user interface requirements and the description of the environment from the ORD.

d. Joint systems must comply with the approved DoD JTA directive (see https://www.disa.mil/). The JTA was established at the direction of the ASD (C3I) in response to the recognition of the need for joint operations in combat given the reality of a shrinking budget. The JTA is binding on all DoD C4I acquisitions to ensure that they are both joint and interoperable. The JTA-Army is a subset of the JTA and provides a comprehensive set of standards required for both Intra-Army and joint interoperability. It provides the baseline of standards with which Army IT capabilities will conform. Compliance with the JTA–A is mandated by 30 Sep 2006 for all Active, Reserve, and National Guard Army systems that produce, use, or exchange information electronically.

e. Other sources of information for the system evaluator concerning the overall interoperability of a system are test reports furnished to the PM by the JITC. JITC functions as DoD's joint interoperability certifier. CECOM SEC APTU serves as the Army's focal point for the joint certification of Army systems and, as part of the APTU responsibilities, prepares these test reports. There are many references to specific software in the JTA that may be obsolete or not easily integrated into the software baseline. If so, it is incumbent upon the system evaluation to highlight this situation so it can be addressed by the respective Commander-in-Chief Interoperability Program Office or the Joint Forces Command.

O–2. Interoperability system evaluation planning

The interoperability KPP, along with other KPPs, CTPs, and operational issues, is used to develop the TEMP. All systems will undergo interoperability certification testing (see chap 6) prior to the FRP DR. IA hardware and software

capabilities are assessed for and must meet interoperability requirements. As joint interoperability certification authority, the JITC will be actively involved in the joint interoperability system evaluation planning effort. The Army interoperability certification authority is the CIO/G–6. The CTSF at Fort Hood, TX, will be responsible for conducting all intra-Army interoperability testing. Prior to joint certification, all Army systems must undergo Intra-Army Interoperability Certification at the CTSF and obtain Interoperability Certification by the CIO/G–6.

a. Interoperability benefits typically manifest themselves in improvements to system performance metrics (see fig Q1). Decreased time to perform a function, increased number of target opportunities, and more precise or timely information are examples of how interoperability can be quantified. These metrics are often expensive in that they require a base case against which to measure the increase or decrease in performance. Interoperability also enhances the warfighters' capability to minimize fratricide.

b. Interoperability also manifests itself in a negative way by increasing the time required to begin or complete missions. In addition, interoperability may require the handling and transport of additional equipment, as well as extra operators and maintainers. The system evaluator quantifies these effects and uses the metrics produced to provide a value judgment on the operational effectiveness of the system. The system evaluator must also address the time required to restore lost interoperability as well as the impact of the loss. When appropriate, interoperability shortfalls will be given an equal amount of emphasis and priority as internal system shortfalls.

Appendix P

Natural Environmental Issue: System Evaluation Considerations

P–1. Overview of the natural environment

An Army objective is to develop systems that will perform adequately under the environmental conditions likely to be found in the areas of intended use. The climatic conditions, as well as performance standards for operations, storage, and transit for each system, are specified in the ORD and the life cycle environmental profile or specifications. The necessity of testing systems in climatic chambers and at desert, tropic and arctic test sites to support the system evaluation is determined by review of these requirements and according to Army policy.

a. Systems will be tested and evaluated for their ability to remain safe, effective, suitable, and reliable in those environments in which they will be stored, transported, handled, and operated. Natural field environments, such as those at ATEC test centers that represent conditions of the various Climatic Design Types as described in AR 70–38, will be considered in the overall testing of systems to ensure the system will be subjected to the synergistic effects those natural environments provide.

b. Prior to testing in natural environments, testing in climatic chambers will be considered. Results of climatic chamber testing may be used to evaluate the system's ability to satisfy its performance requirements. Chamber tests may also be valuable in assessing the risk associated with not conducting tests in the natural environment. Causes for failure in simulated environments must be resolved before the system is subjected to natural environment testing. Chamber tests and simulations play a significant role in the beginning of the development cycle but must be integrated with testing conducted in real world, natural environments.

P–2. Procedures

The system evaluators aid the CBTDEV and MATDEV in preparation of a life cycle environmental profile as presented in MIL–STD–810. The testers and evaluators help in the identification of expected system performance and reliability in the identified environments based on historical knowledge of similar systems, if available.

a. The testers and evaluators, in coordination with the T&E WIPT, determine which environmental testing is the best means of obtaining the desired performance and safety data. The results obtained from laboratory environmental tests, along with life cycle environmental profile information, is used to determine the need and types of natural environment tests beyond the Basic Climatic Design Type to which the system will be subjected.

b. The TEMP and SEP will identify system characteristics that might be abnormally affected by exposure to natural environments. These documents will also address the requirements to subject the system to those climatic effects that exist in areas of intended transportation and storage, as well as establish the need for long-range life cycle surveillance testing of systems in natural environments. As a minimum, the system evaluators will reflect, as one of their CTPs, the ability of the system to operate in the Basic Climatic Design Type. A rationale is required when not using natural environment testing.

c. These requirements must satisfy the policies set forth in AR 70–38.

Appendix Q

Software Issue: System Evaluation Considerations

Section I

Software Evaluation Planning

Q–1. Importance of software evaluation

Software plays an important role in determining a system's effectiveness, suitability, and survivability. The system evaluator must identify the qualitative and quantitative characteristics of the system's software that will impact the system's capability to support its mission and develop plans to evaluate that software.

Q–2. Software evaluation approach

a. The system evaluator typically uses the CE process to determine the software's capability to support the Army user requirements. Software evaluation determines whether the embedded software meets the system and user requirements. The size of the software development effort and the criticality of the software to overall system mission success usually determine the size and scope of the software evaluation. At a minimum, the system evaluator should ensure that the following activities are included in the system evaluation planning effort:

(1) Identify critical software issues, including the essential software characteristics and critical mission functions that are necessary to accomplish the system's mission.

(2) Verify that quantitative thresholds exist for the CTPs of the software components that implement critical mission functions.

(3) Verify that the software development test cases and test environments are adequate to demonstrate compliance of the software with technical performance requirements.

(4) Confirm that systematic software developmental test is performed under the most realistic conditions possible and provide quantitative data that can be analyzed objectively.

(5) Verify that software evaluations are conducted after each planned test event and that these evaluations are identified in the TEMP and in system evaluation planning documents.

(6) Confirm that an effective software correction process is defined in the developer's contract and in the Software Development Plan.

(7) Ensure that a software measurement program is implemented to support the evaluation objectives and to allow the system evaluator and acquisition managers to make technical and management decisions.

(8) Ensure that the software measurement program provides the quantitative data to verify that the software meets the approved exit and entrance criteria and can support the system operational requirements prior to OT.

(9) Identify the software support activity (SSA) that will assume all the Planning, Programming, Budget, Execution System (PPBES) from the MATDEV dealing with PPSS/PDSS of the system (that is, program development, test, problem correction, training, and fielding efforts).

b. The system evaluator should understand any factors that may inhibit realistic DT or OT of the software (for example, the maturity of the software or the availability of test resources). The system evaluator should understand the impact of the test limitations to verify whether the software can support the system's mission and address the COI. It may be beneficial to perform a risk analysis to determine the impact of such limitations on upcoming test events.

c. The TEMP should document the most significant impact of the software on system user requirements. The critical thresholds that are impacted by software should be defined in Part I of the TEMP. Part I should also list the key software features and components that allow the system to perform its required operational mission, such as architecture, interfaces, and security levels. The TEMP and the ORD describe the system's CTPs, which may include software maturity and software performance measures. The TEMP may also include key software maturity thresholds as exit criteria to proceed to the next level testing. Given that the Army does not require the use of the Computer Resource Management Plan (CRMP), either the ILS Supportability Strategy or TEMP should contain data required to support effective planning of life cycle support for the software product being developed. This information should include all requirements for PDSS/PPSS.

d. The complexity of software functions of most Army software-intensive systems will often require that software be identified as a separate evaluation issue. There are many areas of interest in evaluating software, which are listed in table Q–1. Software MOPs should be developed to address these areas of interest. These software measures provide objective, quantitative, and qualitative data on the technical and management status of the software process and products. Table Q–2 describes potential software measures. These measures should address system-level performance of the software and the impact on the mission.

e. The SEP for a software-intensive system should include the following information—

(1) The relationship between the system CE objectives and the software characteristics that affect the system mission and COIs.

(2) The relationship between the system mission and COIs and the AIs that have been identified for the software.

Table Q–1
Areas of interest in Army software evaluation

Software areas of interest	Definition
Performance	How well the software supports system performance.
Interoperability	The ability of two or more systems to exchange information and to mutually use the information that has been exchanged in an Army, Joint, or combined environment.
Usability	The effort required to learn the user interface with the software, to prepare input and to interpret output of the software.
Reliability	The probability that software will not cause the failure of the system for a specified time, under specified conditions.
Maintainability	The effort required to modify the software.
Safety	How well the software inhibits the system from engaging in unsafe action toward personnel, equipment or materiel.
Information assurance	How well the software safeguards information and handles unauthorized attempts at system or data access.

Table Q–2
Software areas of interest and potential measures

Software area of interest	Potential measures
Performance	
System response time	Conformance to specified time tolerances.
System accuracy	Correctness and defects in system level behavior; how close computations are to expected results.
Recovery/restart procedures	Users can overcome potential processing malfunctions.
Conversion processes	Data handling procedures for left-of-baseline and right-of-baseline processing are described and executed in a correct manner.
Robustness	Legal or illegal operator entries or procedures do not cause system degradation except as allowed in accordance with requirements.
Repeatability	Consistent conditions or events produce consistent results.
Interoperability	
Transmission verification	Acceptance of legal transmissions and rejection of illegal transmissions.
Transmission prioritization	Transmissions sent or received are prioritized and handled in the proper order.
Stress	Data and transaction volumes, loads, varying conditions, or peak processing do not degrade the system except as allowed in accordance with requirements.
Interface considerations	Ease of data handling through cycle processing, intersystem data transfer, transmission of data over communications links, and time sharing links are functioning properly.

Table Q–2
Software areas of interest and potential measures—Continued

Usability	
Efficiency	The software helps users in their mission.
Affect	Users like using the software.
Helpfulness	Prompts and help messages are useful; the software is self-explanatory.
Control	Users can easily control the software and accomplish what they want.
Learnability	Users can easily learn and remember how to use the software.
Reliability	
Downtime	System downtime due to software defects and the impact on the mission.
Time to restore	Amount of time needed to restore system to operable state following a software-caused downing event.
Remaining defects	Probability critical software defects remain in the system, and the projected amount of test time needed to uncover those defects.
Maintainability	
Documentation quality	Adequate degree of completeness, correctness, consistency and understandability of software (S/W) documentation to maintain code.
Code quality	Code quality is measured by programming style (for example, complexity, modularity, or commenting), reserve memory capacity and software metrics.
Computer resources	Memory, processor, storage and network capacity is adequate to allow for anticipated growth.
Safety	
Robustness	Legal or illegal operator entries or procedures, or loss of software capability do not cause system to exhibit hazardous conditions to personnel or materiel.
Vulnerability	Degraded operating modes or recovery sequences do not cause undue safety problems for personnel except as allowed in accordance with requirements.
Information assurance	
Computer network attack, exploitation	Time to detect, react, and restore system in accordance with requirements.
Protection features	Attempts at unauthorized use or manipulation are detected and reported in accordance with requirements.
Vulnerability	Assessment of mission impact if system information is compromised.

(3) The analysis and evaluation criteria that will demonstrate compliance with the software technical performance requirements.

(4) The relationship between the software functions being tested and the system-level test events and scenarios.

(5) The methods and measures that will identify traceability of requirements to test events. Any factors that may inhibit realistic developmental and operational test of the software.

Q–3. Army software blocking

a. In August 2001, policy was established to serve as the Army acquisition policy for the definition, execution, management, and synchronization of Army software intensive programs. The basis for the policy was the need to harmonize requirements across individual systems in order to achieve an integrated and interoperable warfighting capability. The Army elected to implement the system-of-systems software blocking as a means to manage the interdependencies between individual system programs. The policy serves as the software annex to the system-of-systems.

b. Software blocking requires that each system-of-systems block will be certified as interoperable before it is released for fielding. Therefore, software blocking relies upon both formal and informal interoperability testing to ensure that systems individually and collectively achieve the required capability. As a minimum, the Block Execution Management Plan will identify—

(1) Systems participating in developmental interoperability testing.
(2) Points of contact for each of the participating systems.
(3) Test start/stop dates.
(4) Top level description of test objectives.
(5) Locations of testing.

c. The CTSF at Fort Hood, TX, will identify the available windows for block-level developmental interoperability testing. Windows will be identified by their start/stop dates, a description of assets available to support testing (for example, CTSF equipment, facilities, and personnel), and any required remote facility interconnect capabilities.

d. In direct support of block certification and interoperability, formal interoperability testing will be conducted to include DoD or any other formal interoperability tests. Where appropriate, compliance will address areas such as IA verification. The formal testing will be conducted in accordance with the CTSF Intra-Army Certification SOP, DoD, or other relevant interoperability certification policies. Any leveraging of these tests for joint certification purposes by the JITC will be coordinated through the APTU at the CECOM SEC at Fort Monmouth, NJ.

Q–4. Army software measurement

Army policy requires the use of software measures to affect the necessary discipline in software development process and assess the maturity of the software products. The Army also requires that software developers address the following management issues using software measures:

a. Schedule and progress regarding work completion.
b. Growth and stability regarding delivery of required capability.
c. Funding and personnel resources regarding the work to be performed.
d. Product quality regarding delivered products.
e. Software development performance regarding the capabilities to meet program needs.

f. Technical adequacy. Sample measures addressing these management issues can be found in section VI of this appendix, as well as in the Practical Software and System Measurement Guidebook (see https://www.psmsc.com/). The system evaluator must consider balancing the software evaluation needs against the software measures already being collected for the system.

Q–5. Evaluating commercial-off-the-shelf software

DoD policy requires contractors and subcontractors to use commercial items and NDI to the maximum extent possible. The system evaluator should understand the following when addressing COTS-based software:

a. All system components should go through the same system evaluation and test procedures regardless of their origin.

b. COTS vendors are under pressure to release products to the marketplace quickly, sometimes with minimal testing and debugging. Even reputable COTS vendors produce products with defects.

c. Fault isolation in systems with COTS components can be difficult because the system evaluator is forced to make inferences about how the components work based on the system behavior. Failure in a complex system with several interacting COTS components compounds this difficulty.

Q–6. Post deployment software support

PDSS refers to modifications or upgrades made to a system's software following the system's FRP DR and initial fielding. See section VIII of this appendix.

a. The PDSS environment generally focuses on correcting reported software errors, thus enhancing the deployed software performance. The SSA organization conducting PDSS typically collects these changes into a few formal software releases to minimize the impact on the fielded system. Differences in the amount of change to software and

timing of software releases should be considered in identifying the scope of total T&E required and the extent of T&E team involvement.

b. When independent system evaluations are necessary, the risk analysis procedure outlined in section VII of this appendix can help determine the amount of testing needed to support those evaluations. In general, independent system evaluation is needed when changes in computer resources, such as hardware, software, firmware, or communications—

(1) Have a physical impact on either the operation or support of the system.

(2) Have a noticeable impact on the system's operational effectiveness, suitability, and survivability, affects user interfaces, or impact critical mission functions.

(3) Cumulatively effect 15 percent or more of the software units in the system since the last time such evaluations were made.

Q–7. Post production software support

a. For mission critical computer resources (MCCR), the MATDEV is responsible for all software support until the weapon system hardware production is complete and is responsible for the PPBES activities. A MCCR system will transition into the PPSS phase of its life cycle the first full fiscal year after the weapon system hardware production is complete. The MATDEV will plan, program, budget, and execute all MCCR weapon system software support requirements until the transition of PPBES responsibilities from the MATDEV to the designated SSA is completed. Once the transition is complete, the SSA will assume all PPBES responsibilities for the PPSS of the weapon system. PPSS requirements and funding data will be submitted by system to HQDA. DCS, G–3 prioritization guidance governs the funding of the PPSS. TRADOC will review the DCS, G–3 prioritization guidance and recommend adjustments to PPSS priorities based on near-term battlefield requirements.

b. For non-tactical C4/IT systems, the MATDEV is responsible for PPBES activities for assigned programs until the system is transitioned to the designated SSA. The MATDEV will use the management decision process to program and budget all PPSS prior to transition to the SSA. PPSS requirements and funding data will be submitted in accordance with the CIO process funding and prioritization of non-tactical C4/IT systems.

c. Procurement or RDT&E funds will be utilized for all software support requirements until the weapon system hardware production is completed or in support of significant modifications. Operation and maintenance, Army dollars will be utilized for software support after the weapon system hardware production is complete.

d. Coordination of software block upgrades of new software-intensive systems, under an evolutionary acquisition/spiral development strategy, use RDT&E funds. Fielded increments are maintained though PPSS and use operation and maintenance, Army funds. Software block upgrades and a spiral development process are part of the Army policy for new software intensive systems. The Army's Unit Set Fielding policy seeks to ensure compatibility with other systems in a system-of-systems architecture. Fielded systems that may be components of a system-of-systems architecture, however, are themselves not static baselines but may consist of multiple versions in different units depending on the PPSS schedule. This may result in additional development costs or incompatibilities as a new program releases software block upgrades that can become incompatible with fielded systems due to ongoing PPSS activities.

Section II

Software Evaluation Support

Q–8. Sources of software evaluation support

An ideal software evaluation will assess the software under all possible conditions in the system operational profile. This means that an effective software evaluation must be based on more than the formal OT that takes place at the end of system development. OT rarely includes all the environmental conditions and MPs that are possible for the system. The opportunities for evaluating software during a formal OT are limited to "black box" testing. "Black box" testing assumes that the software functions are correct if system performance is adequate (that is, the appropriate outputs are received from the corresponding inputs). This provides only a limited window into the technical complexities of the software. Therefore, evaluation of a software-intensive system requires an aggressive, early assessment of technical and functional characteristics, using all available sources of data.

Q–9. Modeling and simulation

a. M&S has become an integral part of testing complex systems. Because Army software-intensive systems have grown increasingly complex, T&E of such systems under realistic conditions is difficult, if not impossible, without putting these systems in a real-world environment. The practicalities of cost, test range space, safety, and the

availability of advanced threat systems or surrogates limit the ability to create these realistic conditions. M&S can address such limitations. M&S can replicate those conditions that could not be created in a test environment due to constraints and limitations. M&S also allows the system evaluator to examine a broader set of conditions than those tested, providing a broader understanding of software and system performance. While not a replacement for testing software in the target environment, M&S is typically needed to evaluate complex system software.

b. The system evaluator must ensure that each use of M&S that has an impact on the system evaluation has gone through the required VV&A process to ensure that it provides credible results and satisfies the M&S users' operational needs (see AR 5–11 and DA Pam 5–11). The system evaluator will typically be involved in determining the acceptability criteria for use of an M&S (for example, how closely does the M&S have to reflect reality in order to meet the needs of the evaluation).

Q–10. Spiral development process

DoD policy has established the evolutionary acquisition strategy as the preferred approach for acquiring systems. An evolutionary acquisition strategy encourages time-phased development of technical requirements and supports communications with users. If an evolutionary acquisition approach is not used, DoD policy requires that software development and integration still follow a spiral development process in which continually expanding software versions are based on lessons learned from earlier development. Spiral development is a cyclical, iterative, build-test-fix-test-deploy process that yields continuous improvements in software. The spiral development process provides several benefits in evaluating a system's software, including the following:

a. An opportunity to obtain realistic data to address the system evaluation issues for each increment in the software-intensive system.

b. A more realistic set of user requirements that are derived from an improved software requirements definition process where a small initial set of requirements is refined over time to meet changes in technology and user needs.

c. Relatively small releases of software that are demonstrated in an operational environment, rather than a single, system-level software release.

Q–11. Computer resources management plan

Many Army organizations develop a Computer Resources Management Plan (CRMP) to support acquisition of software development projects. A CRMP is not required by Army policy and may not be available for every project. The CRMP describes the factors needed to support effective planning of a software acquisition project and life cycle support of the software products. A computer resources working group may provide the information that a system evaluator needs to coordinate CE activities with the acquisition community, including life cycle activities and resources to monitor the software development. These activities and resources typically include the software T&E plans and schedules, the development requirements that the system evaluator expects to see in the RFP, the developer's plans for tracking software maturity, and the program manager's plans for addressing software in the OTRR. Other information that may be provided in a CRMP includes the following:

a. Resources to support T&E, such as instrumentation, drivers, stimulators, loaders, facilities, and special test software.

b. The extent of independent verification and validation (IV&V) that will be used in the software development.

c. The software configuration management (CM) program.

d. The software quality program, including failure reporting procedures, metrics, and criteria against which the software products will be evaluated.

e. The level of Government access to contractor software development activities in order to track software development.

f. PDSS responsibilities.

Q–12. Configuration management process

An effective software CM process can provide significant quantitative data to support software evaluation. The CM process defines the current approved software baseline and software design, including interfaces. It also identifies and controls software changes throughout the system life cycle. The CM function implements and maintains the trouble reporting system, and it tracks test results from the lowest level of testing within an organization. Therefore, software T&E requires an effective CM process in order to define software status.

Q–13. Program review process

Information to support software T&E also may be obtained from the project tracking and oversight activity that is implemented by the software development organization. The most common activity is for an organization to establish

a program review process. These reviews provide information on the overall technical and management status of the project. The development organization convenes technical or management reviews that are attended by developer and acquirer personnel to support effective communication, review project status, surface and resolve outstanding issues, and determine and concur on strategies to mitigate identified risks. User representatives should also participate in the review process to provide feedback from the system mission perspective, especially on software functions that have user interfaces.

Q–14. Software working-level integrated product teams

The PM may form a software WIPT to provide experts in software development and system acquisition processes. The software WIPT bridges the gap between Army operational experts and the developer's technical software experts. A software WIPT focuses attention on issues and risks in software acquisition, development, fielding, and support. Software WIPT members should, at a minimum, include a TRADOC representative or user representative, the project or system engineer, and software engineers from the SSA, commonly referred to as the Army life cycle software engineering center (LCSEC), within the MACOM. The SSA participants may provide long-term support with software development expertise and user domain and interoperability experience. The SSA is often the only Army organization that can address many Army software engineering issues, including:

a. Discussing the issues and planning for the risks associated with the software acquisition, development, fielding, and life cycle support.

b. Operational doctrine, reuse, business process reengineering, and domain/architectural issues.

c. Evolutionary improvements, relevant emerging technologies, the state-of-the-practice, and available COTS and Government-off-the-shelf software.

d. Interoperability, continuity of operations, and supportability.

Q–15. Independent expert reviews

Independent expert reviews may also provide a system evaluator with valuable, software-related information. DoD acquisition policy requires independent expert reviews of all ACAT I through III software-intensive programs. An independent expert review team is composed of a small group of software, systems engineering, and technology experts. The team reviews the program and reports on technology and development risk, cost, schedule, design, development, project management processes, and the application of systems and software engineering best practices. The team reports its findings directly to the program manager and the PEO or equivalent management official. If available, these results may provide significant information to the system evaluator.

Section III

Software Evaluation Activities

Q–16. Evaluating software development process

a. The system evaluator should ensure that there has been an assessment of the capability of the organization that is developing the software. This assessment should determine if the organization has an established, mature process for developing software, and whether or not the software project is following the process. The primary purpose of a software process evaluation is to get an early estimate of the quality of the software products to be delivered based on the maturity of the organization's development process. The software process evaluation also—

(1) Provides a better understanding of the software developer's processes and techniques for building and testing software.

(2) Provides early identification of problems that could potentially lead to operational risks.

(3) Forecasts cost and schedule slips.

(4) Helps the system evaluator understand the inherent software risks to support T&E planning. The system evaluator may choose to participate in a formal software process assessment. In most cases, however, the system evaluator will have to rely on assessments that have been performed by other organizations or self-assessments that have been made by the development organization itself.

b. Army acquisition policy also requires a software capability evaluation of a potential developer for a software development contract that meets specified criteria for size, cost, and criticality. An software capability evaluation is a formal assessment of an organization's software process capability, according to the Software Engineering Institute (SEI) Software Capability Maturity Model (CMM). DoD policy also requires that contractors for ACAT I or IA programs undergo a software process evaluation using the CMM, or equivalent, with a goal of being rated at CMM level 3.

Q–17. Evaluating software requirements

A system evaluator should begin the evaluation of the software requirements by reviewing the process that was used to define them.

a. Software requirements are derived from user requirements. The first step in the development of all systems is for a user representative to define and document the user requirements that must be implemented for the system to achieve its mission requirements. Software will then be designed to implement the user requirements through internal, automated commands. An accurate and complete set of user requirements is the foundation of effective and suitable software.

b. The developer then draws on the user requirements to define and document the software requirements. Software requirements include the functional, performance, physical, interface, and other requirements that must be achieved for the software to support the system. This step includes documenting the methods that will ensure each requirement has been met.

c. The process used to define the software requirements often has the greatest impact on the level of reliability that will be achieved in the final software product. Figure Q–1 provides more information on prediction of software reliability during a software development program. The quality of a software requirements definition process is determined primarily by the skills of the people who define each level of the software requirements. Skill factors include the level of familiarity with user requirements, the ability to document these requirements, and the ability to translate these requirements into system contract specifications. These "quality factors" usually are best defined in qualitative, not quantitative, terms.

d. Evaluation of the software requirements should also be performed through a series of individual specification assessments, informal walk-throughs, or formal reviews. Specific activities may include—

(1) Review of the system's mission and top-level design specifications to determine whether adequate analysis and understanding of user inputs, feedback, and needs ensure that system requirements are accurate and complete.

(2) Assessment of requirements testability to verify that the ability to collect performance data during system-level tests, including formal Government tests, is addressed.

(3) Identification of the maximum usage and stress levels on the system computer resources to define the design limits for software resources, such as timing and memory utilization.

(4) Evaluation of the requirements to determine the degree of completeness, traceability, and stability.

(5) Evaluation of the process to ensure traceability between system requirements and the hardware and software configuration items (CIs) comprising the design.

(6) Analysis of applicable metrics, such as requirements traceability and requirements stability.

Q–18. Developmental testing of software

The DT program must provide assurance that the software meets the system requirements before entering OT. Therefore, the system evaluator must ensure that the software development program includes effective T&E activity. The software development process must provide continuous product evaluation through the analysis of system requirements, software design, and the translation of the design into functional code. To ensure that a software design is adequate to begin OT, the system evaluator must ensure that adequate "static" analysis has been performed. Static analysis refers to evaluation procedures that are employed without requiring the actual operation of the software. Static analysis methods that may be implemented by a PM can be classified as V&V and formal program reviews and audits.

Q–19. Corrective action process

a. Every software developer and maintenance activity must implement a corrective action process to manage the problems that are detected in the approved software product baseline. The corrective action process must be a "closed loop" process in which software problem change reports (PCRs) are written on all detected problems, monitored in a tracking and reporting system, and marked as closed when the problem is corrected. The same procedures apply for both hardware and software PCRs. PCRs are sent to the CCB to be scored and determined if and when they should be addressed. Several PCRs are usually bundled into an engineering change proposal (ECP) when changes exceed current planned cost/schedule estimates.

b. It is important for the system evaluator to understand the software PCR process because PCRs are the most common measure of software product quality. PCR is the formal description of any problem observed in an "approved" software product that has completed some level of evaluation and has been placed under configuration control. Other common terms for a PCR are software trouble report (STR), software problem report, and software problem. A PCR not only identifies problems, but also tracks the status of problems until they are resolved. A software PCR can be written and submitted by anyone, including system developers, system operators, testing personnel, maintenance personnel, or installation, integration, and production personnel. Section IX of this appendix provides a

detailed description of the software PCRs and the process for managing PCRs. Section VI provides the fault profiles measure that is used for tracking PCR status.

Q–20. Software unit evaluation

a. Unit test records are routinely produced by the software developer's CM agent. If metrics are reported on unit testing, the system evaluator may review the data to gain early insight into the software development effort. Unit test is the first and lowest level of functional testing that is executed during a software development effort. Unit test is an informal test and a byproduct of the detailed software design process. The junior programmers who produce the units of code typically receive the first approval of the detailed unit design from their peer review group or chief programmer team. After design approval, the junior programmers write the code for the unit and check the single unit function in a unit test.

b. Unit test records usually report only the number of unit tests that have been passed. To be able to evaluate unit test records, the system evaluator must understand the completeness of the project's unit test criteria and the capability of the CM agents to manage the process. The system evaluator will usually not review records of the software developer's individual unit test cases and test results. Review of individual unit records is often too extensive for an independent evaluation; it is usually performed by a developer's independent quality assurance group or the Government's software quality assurance or V&V agent. The software developer's independent quality assurance group can be by choice or as a requirement for ISO certification. To maintain the ISO 9000 certification, a software developer must have an independent quality assurance group that periodically audits the development process. Independent in this instance means corporate in-house but external to the project being audited. ISO 9000 certification can provide the system evaluator a measure of confidence to the quality of the software development effort.

c. The system evaluator can gain additional insight by understanding the unit design and test criteria. Unit design and test criteria provide information on the quality of the developer's test program and software products. Examples of these criteria are requirements for design modularity and complexity. Modularity measures the characteristics of software design that ensure functions are independently achieved in each unit of code. Modularity supports functional independence and traceability of code units and enhances the developer's ability to find problems in specific units during test. Because the defective units are functionally independent, they can be fixed and replaced with a lower risk of introducing other problems in the software. Software complexity is most commonly measured as cyclomatic complexity, or the number of independent control paths, from entry point to exit point, that can be executed through a software design unit. A lower number of independent paths require fewer tests to exercise all possible control sequences in that piece of software, resulting in software with fewer faults.

d. The system evaluator can also use the CM records of the number of approved design units to determine the level of design stability that has been achieved. The design stability measure tracks the number of changes that have been made to the approved baseline design of the software. A higher design stability measurement indicates a better chance of the software achieving a stable test configuration during the development effort. A stable configuration allows the developer more time to test and debug the software product that will be delivered. The design stability measure may be monitored by the system evaluator to determine the number and potential impact of design changes, additions, and deletions on the software configuration. The trend of the measure over time indicates whether the software design is approaching a stable state. When design changes are made to the software, the impact on previously completed tests must be assessed. Tests may need to be run again with modifications to test data and conditions.

Q–21. Unit integration evaluation

a. First testing results. Software unit integration test typically provides the system evaluator with the first software DT results. Although the first software tests are performed at the unit level, these tests are not formally reported or identified with a pass/fail status. During unit integration, the developer integrates two or more software units and tests the composite package to ensure it meets the functional specifications. The developer successively integrates software units until a complete software CI has been tested. The objective of unit integration and test is to produce a software CI that has been verified to achieve all specified functions for that item. The system evaluator may find that the data on unit integration and test are formally collected and analyzed by an independent third party who is either part of the developer's organization or an agent who is hired by the acquisition customer. These third-party agents may be responsible for performing software quality assurance or V&V of the code.

b. Fault profile data.

(1) Unit integration test provides useful fault profile data for the system evaluator's assessment. The Army's fault profile metric, which is described in both figures Q–1 and Q–4, measures the number of software PCRs that have been written and submitted to the developer's corrective action system. The fault profile metric also measures the number and type of deficiencies in the current approved software baseline. Each problem is classified according to

the criticality and impact on the system and user, assigning priority levels of 1 through 5 for the most critical through the least critical. Problem reports are also classified according to the type of error, such as requirements, design, code, documentation, or "other." This measure may also indicate the developer's ability to identify and fix faults, if the time to correct problems is also monitored. Any high priority problems should be fixed as quickly as possible. Not every fix will eliminate the original problem; the fix may even cause new problems in the overall software package. All code that is created to fix a problem must pass all the levels of test that are required for new code.

(2) A system evaluator should be aware of the gap between open and closed faults throughout the entire project, especially during testing toward the end of the development effort. Preferably, there should be no open priority 1 and 2 software PCRs from previous testing prior to initiating DT. Moreover, there should be no open priority 1 or 2 software PCRs from previous testing prior to initiating OT. Problem reports that are not corrected until late in the development process often do not receive adequate testing.

(3) A system evaluator should be involved in the prioritization of software PCRs during integration and in the downgrading of any priority 1 or 2 software PCRs prior to any OT. A system evaluator should consider any late fix to a software problem to be a potential risk to software quality and operational reliability of the system, as well as the upcoming OT.

c. Test coverage.

(1) To interpret fault profile data accurately, the system evaluator should not evaluate the data without considering the measures of "test coverage." Error detection is closely tied to the quality of the developer's software engineering and test process. A low number of documented software faults may indicate good processes and products. However, a low number of documented software faults could also happen if problem reports are not effectively collected, or the test program is inadequate. Test coverage metrics are needed to provide a more complete picture.

(2) Test coverage describes the extent to which testing has examined both the functional and physical characteristics of software. Figure Q–1 recommends use of two test-coverage metrics: breadth of testing and depth of testing. The breadth-of-testing metric measures functional coverage, that is, the number of software functional requirements that have been demonstrated successfully. This can be described as "black box" testing, since it is only concerned with obtaining correct outputs from the software, as observed through the system or component. The depth-of-testing metric measures the test coverage that has been achieved on the software architecture. This measure represents the percentage of all possible decision points and paths for control and data flow that have been successfully exercised in the software. This is often described as "white box" testing, since it provides visibility into how the software is constructed. However, it is important to remember that complex systems usually cannot be tested for all functions, because the test environment usually cannot completely duplicate the real-world environment. The system evaluator should understand the limitations of the local test bed and identify those system and software functions that cannot be tested during this activity.

d. Schedule tracking. The system evaluator should also be aware that schedule overruns might lead to shortcuts in software development and test, eventually affecting software quality. The system evaluator can track these problems in advance by evaluating measures of cost and schedule throughout the development effort. Schedule shortfalls often forecast problems with software quality. Cost and schedule overruns during code implementation can only be recovered by saving time and money during the final development phase, software integration, and test. It is easy for well-intentioned, optimistic software developers and their customers to convince themselves that they can save time and money by reducing an integration test program without degrading the quality of the final product. For example, they might shorten an integration test program by performing the same test cases on larger pieces of software than was originally intended. Rather than running a test scenario as each unit is separately integrated into a software build, the test scenario is run once on a piece of code that includes several units. The same test cases are run but on a software package that has a much higher level of complexity. The result is that integration tests will exercise far fewer independent control paths and decision points in the code. The impact on the software reliability is that each untested path and decision point has the risk of undetected errors that may occur during system operation.

Q–22. Evaluating hardware and software integration

a. The final step in the developer's test program usually takes place when the completed software components are integrated with the system hardware. This is typically the last stage of DT performed by the developer before formal Government-witnessed testing of the software. This integration test phase should be performed with equipment that is exercised under conditions that are as realistic as possible. This is one of the last opportunities for the developer to find and fix software problems that may be induced by unanticipated real-world conditions.

b. The system evaluator should be aware of any software-driven system functions that cannot be tested in this final phase of the developer's test program. An effective test process ensures that the most critical software functions are tested, but budget and equipment limitations may preclude testing all functions. These untested software functions

may be an area of high risk for reliability. The system evaluator should also take into account the criticality of those untested functions to both the system and the user.

c. The system evaluator should be aware of the meaning of the test numbers that are reported. For example, each number that is reported for the breadth-of-testing metric represents a single software functional requirement that has been demonstrated successfully. However, the criteria for success are defined by the developer's test plans. A minimal test plan will require only that a single input and single control path be executed for the software to produce the proper function. A more effective test plan would require that the software produce the proper function with several inputs, including extreme boundary-value inputs and concurrent stress loading of the computer. The system evaluator who does not understand the criteria for functional test success cannot assess the risk of software functions failing after delivery.

d. The system evaluator must also understand and assess the selection of "white box" test cases and criteria. Exhaustive testing of all control and data flow paths in software is impossible. The time that would be required to test all possible combinations of software paths is usually longer than the useful life of the system. Therefore, software test planners must be smart in selecting their "white box" test cases and success criteria. Established criteria for the depth-of-testing metric usually require that software structure be considered to be adequate only after passing test cases that will exercise a "realistic" number of paths. The criteria usually require that all software decision points ("if X, then Y") be tested at least once and that tests be conducted under both representative and maximum stress loads.

Q–23. Evaluation of software qualification test results

a. The system evaluator should review the software qualification test plans and results to determine the level of realism and test coverage. The SQT is the first formal, system-level test. The objective is to demonstrate to the developer that the software CI meets its requirements as specified in the contractual system, software, or interface requirements. The demonstrated requirements may include both functional and physical characteristics. A representative for the customer should witness each test to verify contractual compliance. The system evaluator should assess the test cases and test environment for the ability to induce the data and processing loads that are stated in the OMS/MP.

b. Note that formal system-level tests provide only negative assurance of software reliability. Because system-level tests are performed at the highest level of software complexity, they usually achieve very low functional and physical coverage. This is especially true during the relatively short software and system qualification tests that are witnessed by the customer. Because the sample of software paths and functions is small, software errors that are observed in a formal test indicate the likelihood of many more unobserved software errors in the code. In other words, if software problems are observed during a system-level test, the system evaluator can be assured that the risk of many more software failures is high.

c. Finally, the system evaluator should understand that quality cannot be "tested into" any product, especially software. More testing does not necessarily ensure better quality. Dynamic, system-level tests are the best tool for validation of a software-intensive system. However, this level of test must be cost-effectively planned and implemented to provide the widest possible test coverage of the software products. As a method to achieve high-quality and reliable software, dynamic tests should be viewed as a tool for confirming the absence of faults, rather than the preferred tool for detecting faults.

Q–24. Software maintenance and support issues

The system evaluator must evaluate the maintainability of the software and certify that all resources necessary for maintenance, PPSS, or PDSS are available and consistent with planned support concepts. To do this, the system evaluator should evaluate the following characteristics:

a. The life cycle support agency is prepared to assume the life cycle maintenance of the software.

b. The requisite tools, facilities, and instrumentation have been developed and provided to the life cycle support agency.

c. The requisite software documentation has been prepared and evaluated by the life cycle support agency as adequate to support their maintenance responsibilities.

d. The configuration management procedures have been practiced by the software contractor and planned by the life cycle support agency.

Q–25. Software usability and manpower and personnel integration issues

a. Software usability is the adequacy of the Soldier-software interface. The Soldier-software or user-system interface usually is evaluated for two characteristics—

(1) "User friendliness" of the interface.

(2) Adequacy of the system backup modes that can be used when a software function is lost.

b. Various methodologies exist for evaluating software usability, such as the Software Usability Measurement Inventory (https://sumi.uxp.ie/index.html). The chosen method should be tailored to the complexity of the system, requirements of the system, and the life cycle phase. Ultimately, the evaluation is based on the human-factor characteristics of the user-system interface and their impact on system mission performance. User-friendly features of the software interface will influence various factors in software operation, such as the number of operator response errors, the speed of operation, and the level of required training. Operator workload can be measured in terms of the maximum rate of actions or decisions required during peak periods, and the time needed to enter required data or give instructions for specific functions, as well as the impact on the mission. The system evaluator must determine quantitative and qualitative measures to assess these characteristics of the software interface.

c. The adequacy of the software backup modes is usually measured by the mean time that the system is down or operating in a degraded mode with a subjective assessment of the impact on the mission. Software interface problems are also addressed with a subjective assessment of their impact.

Q–26. Safety issues

a. System safety addresses the possibility of catastrophic system failure that could compromise the safety of people or property, or result in mission failure. Software safety must be evaluated only in the system context. Software has no inherent dangers, but systems that are controlled or monitored by software may experience failures that are caused by software and have safety impacts.

b. The system evaluator should identify the software components that control safety-related functions and give them special attention. Software safety activities should be initiated on that component and continued through the requirements, design, code analyses, and testing phases. The system evaluator also might identify the need for a more formal evaluation of software safety, based on the probability that the software might cause or fail to prevent failures in a safety-critical system component.

c. The system evaluator should also consider nonconformance of the software functions with the software requirements. Safety hazards may arise in software-intensive systems when the software requirements are incorrect, inappropriate, or incomplete.

Q–27. Information assurance

a. The system evaluator must ensure that software is evaluated, independently tested, and verified to ensure it meets the minimum standards for security and reliability prior to release for operation. Developers of software-intensive Army systems must include appropriate security features in the initial concept exploration phase of the life cycle system development model. All software packages providing security services must either have appropriate evaluation/certification prior to use, or be selected from the National Security Agency Information Systems Security Products and Services Catalog. Other evaluated software products may be used based on a valid justification and approval from the designated authority. Agencies responsible for distribution of software security products will ensure their evaluation and certification.

b. IA is defined as the capability to ensure the confidentiality, integrity, and availability of information processed by the Army's information-based systems. IA includes security of information and related systems, and both the physical and procedural characteristics of software and hardware. IA characteristics of software must be evaluated to ensure that the security features, practices, procedures, and architecture of the software accurately mediate and enforce the system security requirements. IA recognizes that interconnected systems create shared risks and vulnerabilities where an intruder only has to penetrate the weakest link in order to exploit the entire network.

c. Army policy requires that all information systems and networks must be subjected to an established certification and accreditation process that verifies that the required levels of IA are achieved and sustained. Only Army-approved IA products are authorized for use in an information-based system acquisition. Information systems and networks will be certified and accredited per DITSCAP (DoD Intelligence Information Systems Certification and Accreditation Process) for systems that process sensitive compartmented information. The DITSCAP process considers the system mission, environment, and architecture while assessing the impact of the operation, or loss of operation, of that system on the Army's information infrastructure or the DoD Intelligence Information Systems Certification and Accreditation process (for systems that process sensitive compartmentalized information).

Q–28. Software evaluation prior to operational testing readiness review

a. The following guidelines are provided for the system evaluator to ensure that a software-intensive system development effort is ready for an OTRR:

(1) Ensure that records of all contractor software development tests are available in a summary format, including the results of software error prediction models that may have been applied.

(2) Ensure that the developer can present objective, quantitative data to verify the level of software maturity that has been achieved.

(3) Verify that the software baseline that will be frozen for use in OT has no critical software errors remaining and that records are available to validate the developer's software error corrective action review process.

(4) Ensure that DT exit and OT entrance criteria have been defined for the software, and have been met. All priority 1 and 2 software problem reports that will affect the upcoming OT should be closed prior to start of OT for software-intensive systems.

(5) Ensure that software readiness is a formal agenda item in the system OTRR.

b. The system evaluator may find it useful to conduct a more formal risk analysis to determine the likelihood that the system will encounter problems during the upcoming OT, and the impact of those problems. Paragraph Q–53 provides procedures for conducting this risk analysis.

Q–29. Software evaluation during operational testing

a. The system evaluator must understand the relationship between the software functions being tested and the system-level test scenarios. Understanding this relationship requires a record of the traceability of the system requirements to the software design and the OT cases. This record can be provided by the data collected for the requirements traceability metric that is defined in section VI.

b. The system evaluator should also understand the relationship of the load levels on the tested software to the required operational environment. The software load levels should approximate realistic system operating conditions. Examples of load levels on software are the rate and volume of data transfer, degree of concurrent software tasking, and processor or memory utilization.

c. Complete and consistent treatment of all operational requirements for a software-intensive system is not always possible. The system evaluator must prioritize the system requirements from an operational perspective and limit the test scenarios to those requirements that are sufficiently critical to need definitive validating and tracking. This prioritization is based on the criticality of the operational requirement and the frequency with which it will occur in the field. For example, an OT scenario should exercise the software functional requirement for Control Network Management but may not exercise the software function that provides a memory of operator inputs during a certain time period. The OT scenario must test those system functions that are implemented or impacted by the software and that must be tested and fully validated before the system can be considered suitable for deployment.

d. The software product baseline that has been certified by the developer's quality assurance and CM processes must not be changed with patches or version upgrades during OT, unless severe problems are encountered that may prohibit completing the test. Changes to the software baseline can be made only if each change is acknowledged and approved by the MACOM commander. Any changes to software during OT must be supported by an evaluation of the impact of the change on the consistency of data that is collected by the test. If the software baseline is modified during the test period, the system evaluator must ensure that regression testing has been completed according to the developer's test plan for all new software. Regression testing will verify that the detected problems were actually corrected and that additional problems were not introduced into the software.

e. If the number of priority 1, 2, or 3 PCRs that are experienced during OT become excessive and impact the test objectives, the operational tester can suspend or terminate testing in accordance with the policy stated in AR 73–1.

f. Based on the results of the OT, the system evaluator assesses the system's effectiveness, suitability, and survivability with respect to the COIs and related criteria. The system evaluator should base the software evaluation on the effect that observed software errors have on the system's critical mission functions, usually involving system functional errors and system downtime.

g. The testers and system evaluator prepare a SER to convey the results of the OT to the appropriate milestone DR body. Any problems that were discovered during OT should be recorded in a TIR. If the contract allows, those TIRs caused by software problems should also be entered as PCRs in the developer's corrective action system for resolution before final release of the software.

Section IV

Software Fielding

Q–30. Overview of software fielding

a. The developer prepares the products discussed in this section, unless otherwise specified by the acquirer.

b. If a multiple build software acquisition strategy is in effect, planning should identify what software, if any, is to be fielded to users for each build. Software fielding for a build means those actions necessary to carry out the fielding plans for that build.

Q–31. Objective of software fielding

The objective of software fielding is to make the executable software available to users and deliver the manuals and instruction necessary to operate the software. Executable software includes any data files necessary to install and run the deployed software on target hardware, such as batch files and router tables.

Q–32. Software fielding entry criteria

a. An approved software installation plan or equivalent should exist to guide the installation process.

b. The software to be issued should show evidence of successful testing at all appropriate levels, must be accepted by the MATDEV/FP and user, and must have been certified by quality assurance.

c. If materiel release provisions apply to the system, a request for release must be approved prior to actual field use. AR 770–2, AR 770–3, DA Pam 770–2, and DA Pam 770–3 provide more detail on these requirements.

Q–33. Test activities involved with software fielding

Extensive testing is not inherent in preparing software packages for distribution. The products developed here are tested in other activities. Some check out is done during site installation.

Q–34. Evaluation activities involved with software fielding

Users and LCSEC/PDSS personnel should be heavily involved in CE during this activity to—

a. Review the software installation plan to verify—

(1) Installation task descriptions identify the organization that will accomplish the task, such as user, developer, computer operations, PDSS personnel, as well as the quantity of personnel, required skill levels, and installation schedule.

(2) Provisions for scheduling personnel that will comprise the installation team, students for training, computer support and technical assistance, and arrangements needed for facilities, lodging and transportation, if required.

(3) Procedures are adequate and complete for—

(a) Installing the software.

(b) Checking out the installed software.

(c) Initializing databases or other software with site-specific data.

(d) Converting data from the current system.

(e) Performing a dry run of the procedures in operator and user manuals.

b. Review the software version description (SVD) to verify that the exact version of software prepared for each user site is identified. The SVD should provide—

(1) An inventory of materials comprising the version (such as tapes, disks, documentation, and listings) along with applicable handling and security instructions or duplication and license restrictions.

(2) Explicit identification of all computer files making up the version.

(3) A list of all changes incorporated into the version since the previous version.

(4) Identification of any site unique data.

(5) Installation instructions and procedures for determining whether the version has been installed properly.

(6) Information on possible problems and known errors in the version. Instructions for recognizing, correcting, or avoiding these problems should be included.

c. Review technical, maintenance, or other operations manuals providing instructions for users who—

(1) Both operate and make use of the software's results, as in a software user manual (SUM).

(2) Prepare inputs to and receive outputs from the software but depend on others to operate the software in a computer center or other centralized or networked software installation, as in a software input/output manual (SIOM).

(3) Operate the software in a computer center or other centralized or networked software installation so that it can be used by others, as in a software center operator manual (SCOM).

(4) Operate the computers on which the software will run, as in a computer operation manual (COM).

d. Assess the manuals to determine their usability, correctness, and completeness in imparting the procedures necessary to—

(1) Set up the requisite hardware and software environment for use, including communications equipment.

(2) Operate and interpret results from diagnostic features.

(3) Perform mission tasks or computer runs in different operating modes, such as training, restart, emergency conditions, degraded modes, communications failures, manual override, shutdown, or typical conditions.
(4) Identify, document, and report problems or malfunctions.
(5) Recover from, work around, or avoid malfunctions.
(6) Ensure continuity of operations.
e. Assure that suitable user training and support training is planned.
f. Ensure that installation occurs in accordance with the software installation plan.
g. Implement and analyze applicable metrics.

Q–35. Metrics to consider for software fielding

The metrics marked with an X in table Q–3 apply to preparing for software use. Accounting for the cost of performing this activity and tracking a schedule of events, such as site installations and media preparation and distribution, are the only metrics associated with this activity.

Q–36. Decision criteria for software fielding

Representative products, documents, and decision criteria that typically should be met during preparation for software use are shown in table Q–4. Items marked "final" should contain comprehensive material that corresponds to the current build or release.

Table Q–3
Metrics applicable to software fielding

Applies	Metric
X	Cost
X	Schedule
	Computer resource utilization
	Software engineering environment
	Requirements traceability
	Requirements stability
	Design stability
	Complexity
	Breadth of testing
	Depth of testing
	Fault profiles
	Reliability

Table Q–4
Software fielding decision criteria

Primary responsibility	Principal products affected	Decision criteria
S/W developer and Government SCM	Executable S/W files[1] SPS (exec. S/W section) SVD SUM SIOM SCOM COM Applicable information for tech., maintenance or training manuals	Final Draft Final Final (if applicable) Final (if applicable) Final (if applicable) Final (if applicable) Final (if applicable)
S/W developer and PM	Metrics reports	Updates for cost and schedule
MATDEV, materiel release review board	Material release	Approved by applicable decision authority

Table Q–4
Software fielding decision criteria—Continued

Notes.
[1] As identified in the executable software section of the SPS.

Q–37. Other considerations for software fielding

a. The materiel release process assures that Army materiel is suitable and supportable before the MATDEV may transfer accountability and control of the materiel to users. Systems containing software follow this process. Materiel release actions in support of new procurement, reprocurement, and system changes must also be supported by assessments or evaluations conducted by the independent developmental and operational evaluators. A software supportability statement is included in the materiel release package.

b. The following subparagraphs address software changes that fall under AR 770–2 and AR 770–3 materiel release provisions (whether embedded, proprietary, or non-development software). Adding, modifying, or removing software is considered a change.

(1) Software that may significantly change the system's—

(a) Mission function.

(b) Mission capability.

(c) Performance parameters.

(d) Interoperability requirements.

(e) Software architecture.

(f) Maintainability.

(g) Reliability.

(h) Safety.

(2) A block update consisting of software changes of more than 30 percent source lines of code (SLOC), or 30 percent cumulative SLOC changes since the previous materiel release approval.

(3) A block update consisting of a software translation of 30 percent equivalent SLOC to a different computer programming language.

(4) Software that is significantly changed to run on a different computer processor or different computer system configuration.

(5) Software changes that require new test equipment for the user or impact 25 percent or more of the training POI.

Section V

Software Transition

Q–38. Overview of software transition

a. The developer prepares the products discussed in this section, unless otherwise noted.

b. If a multiple build software acquisition strategy is in effect, planning should identify what software, if any, is to be transitioned to the support agency for each build. Software transition for a build means those actions necessary to carry out the transition plans for that build.

Q–39. Objective of software transition

a. This activity's objective is delivery of all end item executable software, associated source files, computer program support manuals, and instruction necessary for the support agent to—

(1) Operate the deployed executable software on its target hardware.

(2) Regenerate the executable software.

b. Executable software includes any data files necessary to install and run the deployed software on target hardware, such as batch files and router tables. Source files, as used here, also include any ancillary data files essential to recreating executable software from source materials.

Q–40. Entry criteria for software transition

a. An approved software transition plan (STrP) should exist to guide the developer's transition process.

b. An updated CRLCMP should exist to guide the support agent's transition process. Elements of the STrP may be incorporated into the CRLCMP by reference to reduce duplication.

c. Physical and functional configuration audits of software products to be delivered should occur prior to the completion of this activity for each build.

Q–41. Test activities involved with software transition

Extensive testing of target software is not inherent in preparing software materials for transition. However, the developer should demonstrate to the acquirer that the deliverable software can be regenerated (for example, compiled, linked, and loaded into an executable product) and maintained using the hardware, software, and facilities identified in the STrP. Some check out is done as part of the support site installation process.

Q–42. Evaluation activities involved with software transition

a. A software maintainability evaluation with subsequent supportability statement is required for materiel release. This is prepared by the LCSEC/PDSS agent.

b. LCSEC/PDSS personnel should be heavily involved in CE during this activity to—

(1) Review the STrP to verify that all resources needed to control, copy, and distribute the software and its documentation, and to specify, design, implement, document, test, evaluate, control, copy, and distribute modifications to the software are identified and described. Resource descriptions include—

(a) Facilities (buildings, rooms, power, safety, and security provisions).

(b) Hardware (models, versions, configurations, manuals, source of supply, and licensing provisions).

(c) Software (names, version numbers, release numbers, configurations, manuals, vendor support, and data rights).

(2) Ensure the STrP provides a schedule for transition activities, addresses training, and identifies number, type, skills levels, and security clearances required for support personnel.

(3) Assure that the SSDD reflects the "as built" system.

(4) Assure that the software product specification (SPS) is complete and up to date.

(5) Review the SVD to verify that the exact version of software prepared for the support site and each user site is identified. The SVD should provide—

(a) An inventory of materials comprising the version (such as tapes, disks, documentation, and listings) along with applicable handling and security instructions or duplication and license restrictions.

(b) Explicit identification of all computer files making up the version.

(c) A list of all changes incorporated into the version since the previous version.

(d) Identification of any site unique data.

(e) Installation instructions and procedures for determining whether the version has been installed properly.

(f) Information on possible problems and known errors in the version. Instructions for recognizing, correcting or avoiding these problems should be included.

(6) Review software maintenance manuals providing instructions for support personnel who—

(a) Program the computers on which the software was developed or on which it will run, as in a computer programming manual (CPM).

(b) Program or reprogram firmware devices in which the software will be installed, as in a firmware support manual (FSM).

(7) As it applies to each support task, assess the manuals to determine their usability, correctness, and completeness in imparting the procedures necessary to—

(a) Set up the requisite hardware and software programming environment.

(b) Operate and interpret results from diagnostic features.

(c) Describe the physical characteristics of the support equipment or target hardware, as applicable, that must be known to perform programming tasks. Examples are word lengths, interrupt capabilities, hardware operating modes, memory attributes, timers, clocks, input/output characteristics, sequencing requirements, and special features.

(d) Install, replace or repair firmware devices including contingencies to preserve continuity of operations when deployed.

(e) Ensure classification security is safeguarded.

(f) Identify, document, and report problems or malfunctions.

(g) Recover from, work around, or avoid malfunctions.

(8) Assure that suitable support personnel training is planned, if applicable.

(9) Assure that a physical configuration audit occurs prior to acceptance of transitioning material identified in the SPS.

(10) Implementation and analysis of applicable metrics.

Q–43. Metrics applicable for software transition

The metrics marked with an "X" in table Q–5 apply to software transition. In addition to cost and schedule reporting, an assessment of software maintenance capability may be appropriate for organic or contracted support organizations whose comparable prior experience is limited.

Table Q–5
Metrics applicable to software transition

Applies	Metric
X	Cost
X	Schedule
	Computer resource utilization
X	Software engineering environment
	Requirements traceability
	Requirements stability
	Design stability
	Complexity
	Breadth of testing
	Depth of testing
	Fault profiles
	Reliability

Q–44. Decision criteria for software transition

Representative products, documents, and decision criteria that typically should be met during preparation for software transition are shown in table Q–6. Items marked "final" should contain comprehensive material that corresponds to the current build.

Table Q–6
Software transition decision criteria

Primary responsibility	Principal products affected	Decision criteria
S/W developer and Government SCM	Executable S/W files Source files SPS SVD SSDD CPM FSM	Final Final Final Final Final ("as built" configuration) Final (if applicable) Final (if applicable)
S/W developer and PM, Government software quality assurance, and Government SCM	Functional configuration audit and physical configuration audit Metrics reports	Final Updates for cost and schedule; SEE if maintenance capability unproven

Section VI

Army Software Metrics

Q–45. Introduction

a. This section provides 14 examples of software metrics that can be used to gather information on the status of software throughout the life cycle of Army software-intensive systems. The 14 examples are provided only to offer the reader a detailed description of common software metrics in various phases of software development. Army managers are encouraged to collect metrics that address the unique issues and information needs of their organizations or acquisition programs. The Practical Software and Systems Measurement initiative provides guidance on the process to derive these other issue-driven metrics.

b. The overall objective of software T&E is to determine the level of maturity that has been achieved in software. Software maturity is a measure of the completeness of the software development effort and the extent to which the

software products have been validated to meet established requirements. These requirements include all established criteria, such as functional performance, quality, and supportability. It is impossible to establish a single methodology for evaluating software maturity, due to the wide variety of acquisitions strategies, systems, and software architectures. However, for each specific system that is evaluated, it is important to have a well-defined process to determine the achieved software maturity at any point in time. Software maturity should be determined by a set of software metrics that provide objective, quantitative data on the software status. Each software management program should define the procedures and metrics that are most appropriate to measure software maturity.

c. Software metrics are only one of many factors to consider when evaluating software maturity. Many activities contribute to an overall evaluation of software maturity. However, the results of all activities cannot all be expressed as quantitative measurements, and qualitative characteristics must also be considered in any software evaluation. Quantitative measurement data, rather than qualitative ratings, should be used whenever possible as the basis to derive information on the status of software. Quantitative measures, or metrics, are more objective and less subject to the opinion or interpretation of the persons who collect and report the data.

Q–46. Policy requirements

a. Previous Army policy required PMs to use and report 12 of the metrics that are presented as examples in this appendix. However, acquisition reform policy precludes PMs from requiring developers to use and report a specific set of metrics. The 14 metrics are presented as examples of measures that have proven useful for managing risk in software-intensive programs. The description of each metric includes a tailoring section with suggestions for alternative implementations. The PMs also have the flexibility to tailor each metric to address their specific information needs or to use data that their software developer already collects.

b. The Defense Acquisition Guidebook encourages PMs to use a software measurement process in planning and tracking the software development program and to assess and improve the software development process and the associated software product.

Q–47. Classification of metrics

a. The 14 example metrics can be mapped to the seven practical software and systems measurement common issues, as shown in table Q–7.

Table Q–7
Army practical software and systems measurement common issues and software metrics

Practical software and systems measurement common issues	Army software metric
Schedule and progress	- Schedule - Development progress
Resources and cost	- Cost - Manpower (optional)
Product size and stability	- Requirements traceability - Requirements stability - Design stability
Product quality	- Computer resource utilization - Complexity - Breadth of testing - Depth of testing - Fault profile - Reliability
Process performance	- Software engineering environment
Technology effectiveness	- Program-specific issues and measures
Customer satisfaction	- All Army example metrics

b. Software development projects typically track the information and collect the data items needed for the metrics described in this chapter. This detailed data, however, is often used only at lower levels of management within a developer's organization. Summaries are not usually reported to higher level managers in a form suitable to support program management decisions. The suggested metric displays presented in this chapter should be annotated with

program-specific information. The resulting information displays will provide program managers with the insight needed to make informed decisions on software management issues. Displays other than those suggested may be appropriate, depending on the decisions to be made.

c. Several metrics are often needed to evaluate an activity or an issue of interest. For instance, to address whether a program can remain on schedule, relevant metrics include schedule, requirements and design stability, development progress, depth and breadth of testing, and fault profiles. Each metric description includes management information and correlations with other metrics where analysis of program issues takes place.

Q–48. Metrics program considerations

In order to gain the most useful insight into software processes and products, the following should be considered when planning a metrics program or when analyzing metrics data—

a. Be sure the metric data definitions are consistent. For example, the definitions for unit, module, function, and lines of code should be established and followed for the project by all involved in collecting and interpreting the metrics.

b. Metric displays should be combined with other qualitative information. Decision makers must consider program issues when analyzing and evaluating metrics data.

c. Metric displays should be used to portray trends over time, rather than placing too much importance on a calculated value at a single point in time.

d. Never use metrics to evaluate personnel. People will focus on manipulating metrics rather than doing their jobs.

e. Metrics can be expensive in terms of resources. Tailor them to use data already available from the software developer.

Q–49. Metrics tables

a. Tables Q–8 through Q–21 contain an example for each of the 14 Army metrics. These tables are intended to assist PMs in selecting appropriate software measures and specify the related data and implementation procedures. This guidance represents only a starting point for selecting and specifying software measures for a specific project. It is recommended that PMs augment and modify this information to meet individual project requirements.

b. Each example software metric table provides two columns of information. The first section, Selection Guidance, provides information to select a metric that is appropriate for a particular project. The second section, Specification Guidance, provides guidance to help define the appropriate data and implementation requirements. The elements of each column are described in the following paragraphs:

(1) *Project application.* Information that helps to identify if the measure is applicable to specific types of projects. The information addresses applicability with respect to the project life-cycle phase, functional domain, and the size, scope, type, and origin (new, reused, and COTS) of the system. This information specifically addresses applying the measure to real-time, data-intensive, and other types of systems. It also identifies the life-cycle phases in which the measure is most useful and the overall use of the measure within Government and industry.

(2) *Process integration.* Helps determine the applicability of the measure to different program and technical management processes. The information addresses particular program management practices, data availability and cost, and other process characteristics.

(3) *Usually applied during.* Defines the applicability of the measure to different system process activities. These activities include requirements analysis, design, implementation, and integration and test. These activities should not be construed to be sequential but can take place during any phase of the life cycle or concurrently during the same phase. The information in this section also addresses the type of data (estimates or actuals) that is generally available with respect to the identified activities.

(4) *Typical data items.* The data items that are typically measured and collected. For example, the Effort measure has the Number of Labor Hours as one of its data items.

(5) *Typical attributes.* The descriptive data on a characteristic or property assigned to a measurement data item that is used to sort and correlate the data in a project. For example, the number of lines of code data item for the Lines of Code measure includes the attributes of language, source, and version.

(6) *Typical aggregation structure.* The structure by which data are organized and aggregated to the project level. The typical aggregation structures are based on the development activity (such as requirements analysis, design, implementation, and integration and test), the components (such as CI or unit), or the functions. The WBS is a combination of activity and component structures.

(7) *Typically collected for each.* The noted activity or design component level at which the developer typically collects the data items for the measure.

(8) *Data items—additional information (optional).* Provides additional information to help specify the data items for the measure or provides alternatives to the specified data items.

(9) *Count actuals based on.* Typical activities or exit criteria for the listed data elements. This information helps to determine when a measure is counted as an actual, or when an activity or event is complete. Normally only one of these options is used.

c. As follows—

(1) *Cost metric.*

(a) Army metric information. The cost metric at table Q–8 reports the difference between budgeted and actual cost for a specific product or activity and answers questions such as—

1. Are project costs in accordance with budgets?
2. Will the target budget be achieved, or will there be an overrun or surplus?
3. What WBS or project elements or tasks have the greatest variance?
4. Will I be able to complete the project on time?

Table Q–8
Software metric—cost common issue—resources and cost

Selection guidance	Specification guidance
Project application - Applicable to any project that uses a cost and schedule system, such as a cost/schedule control system criteria. **Process integration** - Cost and schedule data are required on most large Government contracts; therefore, it is often readily available. This data should be based on a validated cost accounting system using a WBS. - Cost can be difficult to track without an automated system tied to the accounting system. - Cost data provided by the Government tends to lag other measurement information due to time lag associated with formal reporting requirements. - Limited in applicability if costs are planned and expended on a level of effort basis. - Each WBS element should be linked to a software product with measurable criteria for completion of the product. **Usually applied during** - Project Planning (Estimates). - Requirements Analysis (Estimates and Actuals). - Design (Estimates and Actuals). - Integration and Test (Estimates and Actuals). - Implementation (Estimates and Actuals). - Operations and maintenance (Actuals).	**Typical data items** - Planned cost (dollars). - Actual cost (dollars). - Earned value—budgeted cost of work scheduled (BCWS): the sum of the budgets for all WBS elements that are scheduled to be accomplished within a given period of time. - Budgeted cost of work performed (BCWP): the sum of the budgets for WBS elements that were actually completed within a given period of time. - Actual cost of work performed (ACWP): the cost actually incurred to complete WBS elements within the given time period. - Estimated cost at Completion. - Budgeted cost at completion. **Typical attributes** - Organization. - WBS element. - Product. **Typical aggregation structure** - Organization. - WBS element. - Product. **Typically collected for each** - Project or WBS element. **Count actuals based on** - WBS component complete to defined exit criteria. - Product delivery.

(b) Management information.

1. Software cost elements may include any expenditure required to develop or maintain a software product. The key to proper application of the Cost metric is to identify those WBS elements pertinent to software that pose risk to the overall program.

2. Exceeding the budget allocation at any point in a program is cause for concern and investigation. This is easily detected as a variance less than zero (for either cost or schedule). Consistently or increasingly negative values for variances indicate that the system may be delivered behind schedule or may exceed the budget.

3. Cost is associated with all products and activities and can be related to all other metrics. In general, an unfavorable trend in some other metric may adversely affect cost.

4. The Cost metric compares actual software expenditures to the original budget. When assessing overall cost status, however, consider the amount of unfinished work to be done under the remaining budget. Other metrics that show the remaining schedule events, requirements not yet traced and implemented, and number of unresolved software faults provide information about the amount of work remaining. Insight into the risk of achieving software maturity can be derived by estimating the cost of rework to fix faults and to complete the trace and implementation of requirements.

5. Be aware that cost information may arrive as much as 60 to 90 days behind the delivery of other metric data. When evaluating other metrics with cost, be sure that comparable time periods are examined.

(c) Indicators.

1. Figure Q–1 shows a plot of performance in terms of percentage variance from plan. The two measures plotted on the graph were calculated as—

2. Schedule Variance = (BCWP BCWS) / BCWS

3. Cost Variance = (BCWP ACWP) / ACWP

4. Results near zero indicate that the project is proceeding according to plan. Negative results are an indication that the project is behind schedule or over budgeted cost. Positive results indicate the project is ahead of schedule or under budgeted cost. Thresholds of +/10 percent commonly are used to trigger corrective action.

5. Alternatively, the cumulative ratio of budgeted to actual values can be computed as follows:

6. Schedule performance index = BCWP / BCWS

7. Cost performance index = BCWP / ACWP

8. Plotting these measures yields a target value of 1.0 when performance matches the plan.

9. Figure Q–1 indicates that the project has been behind schedule and should have been investigated. It may be related to either actual performance improvement or to the accounting process. Performance for the last 3 months is outside thresholds, indicating that the project is seriously behind schedule and a new plan is necessary.

10. Figure Q–2 is a line chart indicator example showing the cumulative spending plan, planned funding increments, total cost budget, and actual cost.

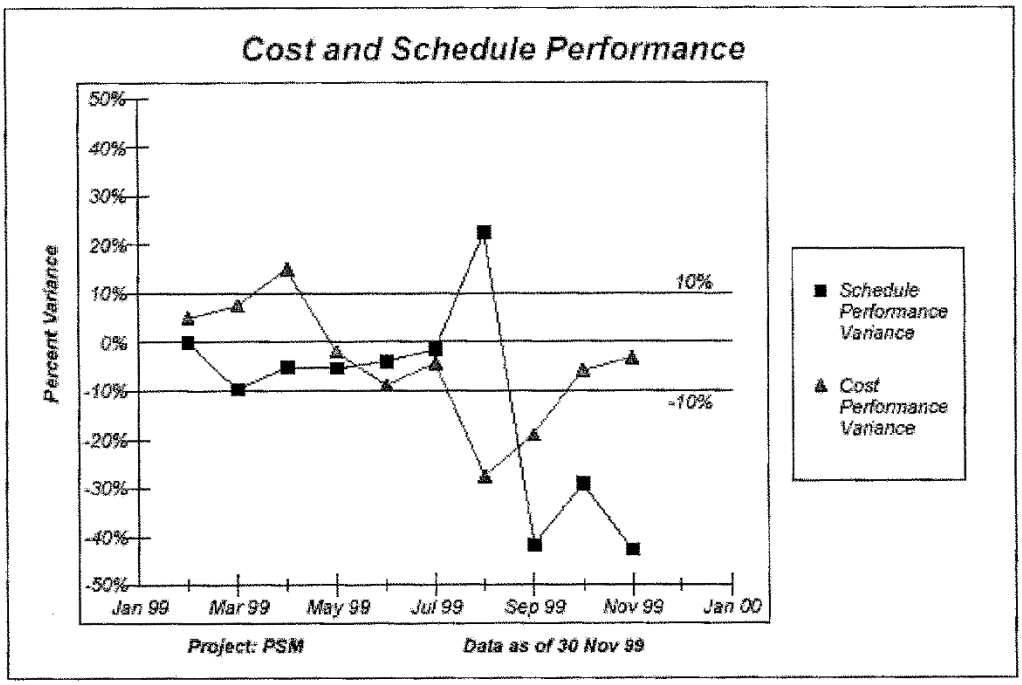


Figure Q–1. Cost and schedule performance

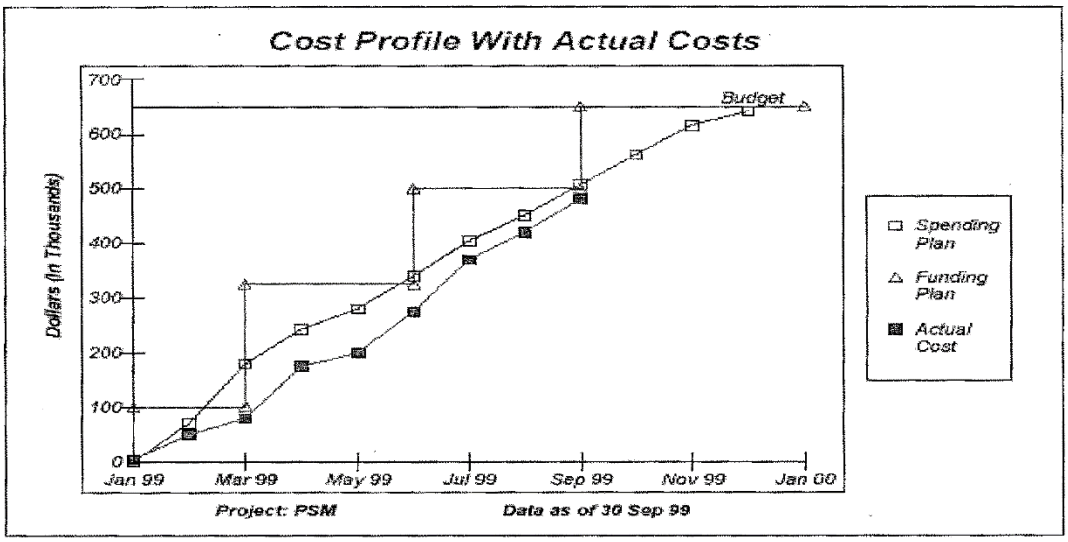


Figure Q–2. Cost indicator

(2) *Software engineering environment metric.*

(a) Army metric information. The software engineering environment (SEE) metric at table Q–9 compares an organization's defined process with the requirements of an accepted reference model. The rating results from an assessment of the organization's process capabilities. A published process model guides the assessment. With the reference model rating and assessment findings, the organization can identify opportunities for improving processes and can measure progress. This measure is sometimes used to evaluate competing suppliers. Staged-view process models provide a single, overall rating for organizational process maturity and a profile of the achieved process components. Continuous-view process models provide a capability rating for each process component that is assessed (rather than a single organizational rating). The quantitative measurement results are limited to the date of the assessment or evaluation and the awarded rating level. However, the most useful assessment information is qualitative, including strengths and weaknesses of various process components. This measure answers questions such as—

1. What is the current process maturity or capability rating of the organization?
2. What process components are established and practiced?
3. What management and technical practices can be improved?
4. Does the supplier meet the minimum process maturity or capability requirements?

Table Q–9
Software metric—software engineering environment common issue—process performance

Selection guidance	Specification guidance
Project application - Normally measured at the organizational level. - Useful for organizations and projects of all sizes. **Process integration** - Rating may be used by the acquirer as a source selection criterion or by the supplier as a competitive advantage. - Applied using a software assessment model. **Usually applied during** - Project planning (Actuals). - Requirements Analysis (Actuals). - Design (Actuals).	**Typical data items** - Date of assessment. - Reference model rating. - Key process areas (KPAs) of the model that were examined. **Typical attributes** - Process identifier. - Reference model identifier. - Project assessed. - Organization. - Assessment type (formal or informal). **Typical aggregation structure**

Table Q–9
Software metric—software engineering environment common issue—process performance—Continued

- Implementation (Actuals). - Integration and test (Actuals). - Operations and maintenance (Actuals).	- Organization. - Activity. **Typically collected for each** - Organization. **Count actuals based on** - Completion of assessment.

(b) Management information.

1. The SEE rating provides a consistent measure of the developer's ability to use modern software engineering techniques in the development process, and therefore the developer's ability to instill such principles and characteristics in their products. The basic assumption to this approach is that a quality process results in a quality product. Other metrics and evaluation techniques should be used to examine product quality.

2. Although software engineers and managers usually know their problems in great detail, they often disagree on which improvements are most important. The SEE metric's use of standard CMM questionnaires allows engineers and managers to focus on a limited set of key processes and work aggressively toward implementing them, rather than being overwhelmed by the total process.

3. The SEE rating assists the acquirer in identifying and narrowing risk to specific areas generally known to have an affect on effective software production. The PM should use the SEE metric to focus on determining developer capabilities and to gauge the ability and willingness of the developer to improve in weak areas over time, rather than using the SEE metric solely to select one developer over another.

4. An assessment often reveals that a developer is proficient in KPAs from a CMM level that is at least one level higher than the rating number assigned. For that reason, the maturity level number is not the only information relevant to appraising actual capability.

5. SEE assessments conducted by an SEI-trained team are desirable. However, acquirers are encouraged to train their staff in determining software development capability and to perform informal assessments themselves.

6. The SEE rating can be used by developers to find and improve weaknesses in their own software development process.

7. Be aware that the SEE metric reflects the developer's practices only at the time of the assessment. Changes in a developer's corporate environment, management philosophy, or other factors may lead to circumstances that detrimentally affect KPAs over time. Therefore, it may be appropriate to conduct an occasional, informal reexamination of KPAs previously judged satisfactory.

8. A higher SEE rating should have a positive impact on all other metrics.

(c) Indicators.

1. Figures Q–3 and Q–4 are examples of SEE metric indicators. Figure Q–3 shows an indicator for a continuous-type SEE model, where each process area is evaluated independently.

2. Figure Q–4 shows an indicator for a staged SEE model, where the maturity level is achieved successfully implementing KPAs, yielding a single rating for the maturity level.

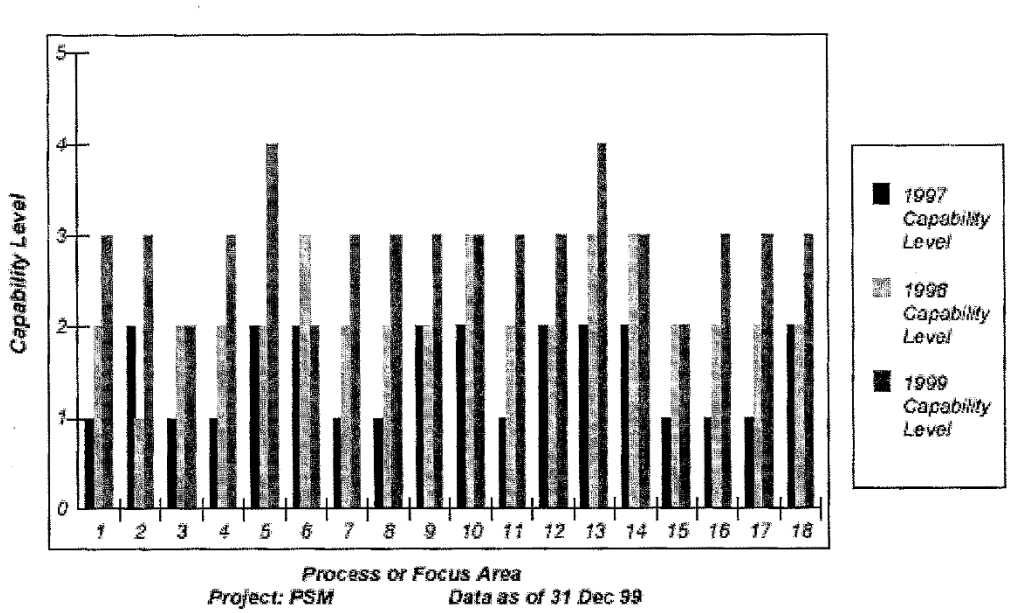


Figure Q–3. Software engineering environment model indicator—continuous type

(3) *Requirements traceability metric.*

(a) Army metric information. The requirements traceability metric at table Q–10 measures the level to which software products have implemented requirements allocated from higher level specifications. Software products include specifications, software design, code, and test cases. This metric answer questions such as—

1. Have all the requirements been allocated to hardware or software components?
2. Are the requirements being tested as scheduled?
3. Is implementation of the requirements behind or ahead of schedule?

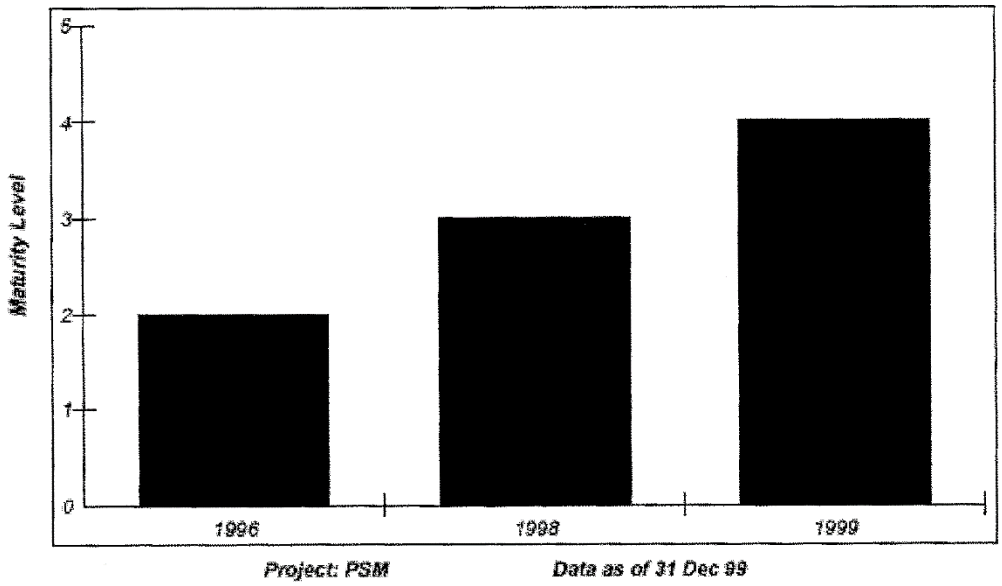


Figure Q–4. Software engineering environment model indicator—staged type

Table Q–10
Software metric—requirements traceability common issue—process performance

Selection guidance	Specification guidance
Project application - Begins with the first specification produced in response to a defined mission requirement. - Applicable when an automated information solution is foreseen and continues throughout the life of the program. **Process integration** - Requires a system-level functional decomposition. - Needs well-defined requirements for system components and interfaces between system components. - It is sometimes difficult to define a "function," but a consistently applied definition makes this metric more effective. -Requirements traceability is verified during Integration and Test. -To reduce risk, prototypes may be used to measure the achievement of design requirements prior to implementation. - Some requirements may not be testable until late in the testing process. Later in software development, the requirements baseline expands, and measurement data are traceable to components and test cases. - Some requirements are not directly testable and must be verified by inspection. **Usually applied during** - Requirements analysis (Actuals). - Design (Estimates and Actuals). - Integration and test (Estimates and Actuals). - Implementation (Estimates and Actuals).	**Typical data items** - Names of the two documents assessed. - Number of system/software requirements in the "traced from" document. - Number of requirements in "traced from" document successfully traced to the "traced to" document. - Number of requirements in "traced from" document that could not be traced to the "traced to" document. - If a backward trace is also performed between the two documents, record the number of requirements in the "traced to" document that were successfully traced back to the "from document," and the number of requirements in the "traced to" document that could not be successfully traced back to the "from document." **Typical attributes** - Name of the two documents assessed. - Software release or increment. - Category of requirement (stated or derived). - Type of requirement (user, system, component, and software). - Importance or priority of the requirement. **Typical aggregation structure** - Software release or increment. - Function.

Table Q–10
Software metric—requirements traceability common issue—process performance—Continued

	Typically collected for each - Software release or increment. - Integration and test (Estimates and Actuals). - Implementation (Estimates and Actuals). **Count actuals based on** - Completion of specification review. - Successful completion of all tests.

(b) Management information.

1. Software test management procedures dictate that software requirements should be traced to their individual qualification test cases. Recording this trace provides visibility to ensure that software requirements are adequately tested.

2. Requirements traceability aids in determining the operational impact of software problems. Failed requirements can be tracked back to specific mission needs.

3. Because of the detailed nature of the requirements traceability metric, collecting the data is most cost effective if it is a normal product of software development or a V&V effort. The record of requirements traceability should be part of the developer's deliverable technical data package.

4. The record of requirements traceability is normally prepared by the software developer, but should also be verified by an independent organization, such as an IV&V agent or LCSEC/PDSS personnel prior to software transition.

5. The PM and user representative may also want to evaluate the record of requirements traceability. This evaluation can be intensive in time and effort, but it is worth the cost when problems or discrepancies are discovered and corrected early.

6. When evaluating the record of requirements traceability, consider the criticality of the requirement to the system user and the criticality of the resultant software function to system operation. A formal method may be used to identify requirements that address key user operations or critical system functions. Another method is to identify the units that appear most often in the record of requirements traceability. These units represent crucial, basic, software functions because they are needed for multiple system requirements. These units can be developed earlier and be given increased test scrutiny.

7. Incremental or evolutionary acquisition strategies, such as rapid prototyping, where all requirements are not known in advance or specified to the same degree of detail, require the tracing of requirements to be an iterative process. As new requirements add more functionality to the system, the record of requirements traceability is revised and augmented.

8. The record of requirements traceability can be a valuable management support tool at system requirement, design, or other joint reviews. It may also indicate those areas of software requirements or design that have not been properly defined.

9. The PM should establish requirements traceability thresholds for proceeding from one activity to the next. For example, a threshold may be defined as some percentage of system requirements specification (SRS) requirements that need to be traced to detailed design before coding begins. Required levels of traceability should be based on the degree of risk assumed for requirements that are not traceable to this point. Individual thresholds are system specific.

10. During PDSS, if a function is modified, the record of requirements traceability can be used to focus regression testing on particular computer software configuration items (CSCIs)/units.

11. This metric does not provide information on whether tests have been executed or on the pass/fail status of specific requirements. The record of requirements traceability can be tailored to include test result status if desired.

(c) Indicators. Figure Q–5 is an example of tracing the SRS to the software requirements specification, CSCI design, unit design, code, and test cases.

(4) *Requirements stability metric.*

(a) Army metric information. The requirements stability metric shown in table Q–11 indicates the degree to which changes in the software requirements or changes in the developer's understanding of the requirements are affecting the development effort. It also allows for determining the cause and source of requirements changes and answers questions such as—

1. Have the requirements allocated to each incremental delivery or increment changed?
2. Are requirements being deferred to later increments?
3. How much has functionality changed and which components have been affected the most?

4. Is the number of requirements growing? If so, at what rate?

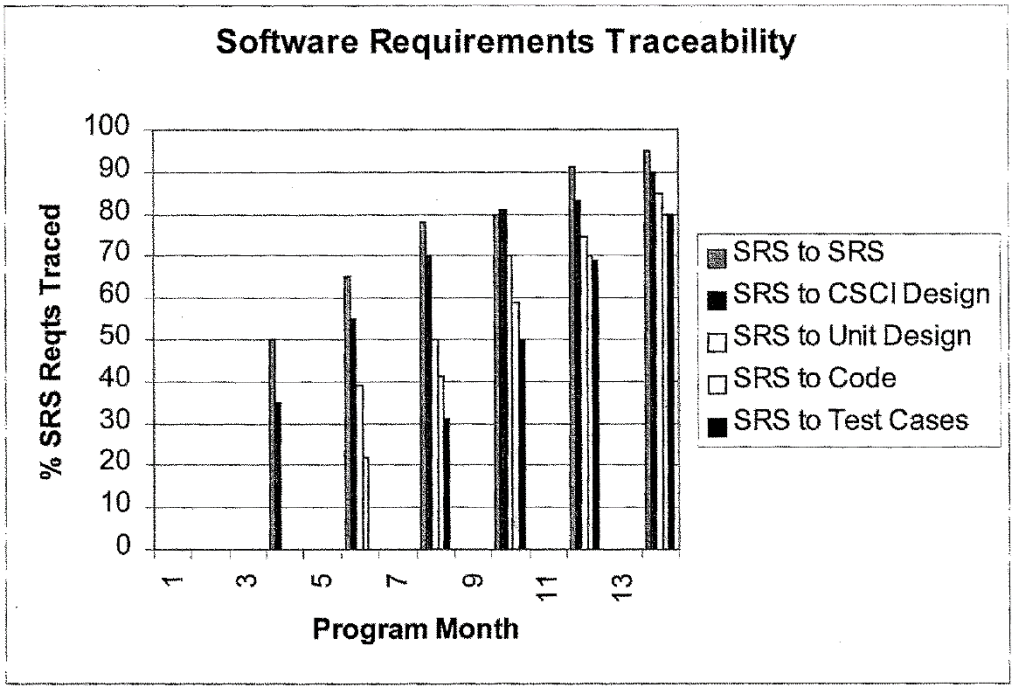


Figure Q–5. Software requirements traceability

Table Q–11
Software metric—requirements stability common issue—product size and stability

Selection guidance	Specification guidance
Project application - Data collection can begin with approval of the MNS and during the system requirements analysis activity. It continues for the life cycle of the system. - Monthly reporting is recommended. **Process integration** - Sometimes difficult to specifically define discrete requirements. A consistently applied definition makes this metric more effective. - Requires a good requirements traceability process. - Count changes only on a baseline that is under formal configuration control. - A description of the impacts (cost, schedule, and functionality) of each change is required. **Usually applied during** - Project planning (Estimates). - Requirements analysis (Estimates and Actuals). - Design (Actuals). - Implementation (Actuals). - Integration and test (Actuals). - Operations and maintenance (Actuals).	**Typical data items** - Software requirements discrepancy status (cumulative total detected and cumulative total resolved). - Total number of SLOC. - Total number of SRS requirements. - Number of requirements added due to approved engineering change proposals—software (ECP–Ss). - Number of requirements modified due to approved ECP–Ss. - Number of requirements deleted due to approved ECP–Ss. - Number of SLOC affected by approved ECP–Ss (proposed by user/proposed by developer). - Number of software units affected by approved ECP–Ss (proposed by user/proposed by developer). - Number of ECP–Ss generated from requirements changes (proposed by the user/proposed by the developer). **Typical attributes** - Increment. - Change source (supplier, acquirer, user). - System component. - Priority (high, medium, low). - Level of requirement (user, system, software).

Table Q–11
Software metric—requirements stability common issue—product size and stability—Continued

	Typical aggregation structure - Software release. **Typically collected for each** - Software release. - Requirement specification. **Count actuals based on** - Passing requirements inspection. - Release to configuration management. - Software CCB approval.

(b) Management information.

1. When a program begins, the details of its operation and design are rarely complete, so it is normal to experience changes in the specifications as the requirements become better defined. Prototyping can help alleviate this problem, or at least trigger refinement earlier in development. When technical reviews reveal inconsistencies, discrepancy reports are generated. Modifying the design or the requirements to alleviate a problem results in closing the associated discrepancy report. When a change is required that increases the scope of the system, an ECP–S is submitted.

2. Allowances should be made for lower requirements stability early on in cases where prototyping is used. At some point, however, the requirements should be firm enough that only design and implementation issues will cause further changes to the specifications.

3. The plot of open discrepancies can be expected to spike upward at each review and to diminish thereafter as the discrepancies are closed. High requirements stability is indicated when the cumulative discrepancies curve levels off, as most discrepancies reach closure.

4. For each engineering change, the amount of software affected should be reported in order to track the degree to which ECP–Ss increase the difficulty of the development effort. Only those ECP–Ss approved by the CCB should be tracked.

5. The amount of SLOC is somewhat dependent on both the application language and programmer style. The key is to watch for significant changes to SLOC due to requirements changes.

6. The PM should establish thresholds for requirements stability before proceeding from one activity to the next. For example, after joint technical review of the software requirements, the requirements should be stable enough to allow coding to begin.

7. The PM should also establish time frames for closing requirements discrepancies. Cost and schedule impacts may be noted when requirements discrepancies remain open after 30 days.

8. Causes of program turbulence can be investigated by looking at requirements stability and design stability together. If design stability is low and requirements stability is high, the transfer from design to code is not working well. If design stability is high and requirements stability is low, the transfer from the users to the designers is not working well. If both design stability and requirements stability are low, neither process is working well.

(c) Indicators.

1. The line chart in figure Q–6 shows two pieces of requirements-related information. The top line is the trend in the total number of requirements defined to date. The bottom line represents the total number of changes made each month (the number of requirements added, changed, and deleted during the month).

2. A bar chart, such as the one shown in figure Q–7, provides more detail about whether the changes were additions, modifications, or deletions.

(5) *Design stability metric.*

(a) Army metric information. The design stability metric at table Q–12 is composed of two measures. The design stability measure tracks changes made to the design of the software. The design progress measure shows how the completeness of the design is advancing over time and provides a context for viewing the design stability measure in relation to the total projected design. This metric answers such questions as—

1. Have changes in functional requirements caused the software design phase to exceed the original schedule?
2. Are design changes implemented as requirements changes are approved, or being deferred to later increments?
3. What percentage of the design has changed since the last formal software release?
4. What components have been affected the most by design changes?
5. Is the software design phase on schedule?

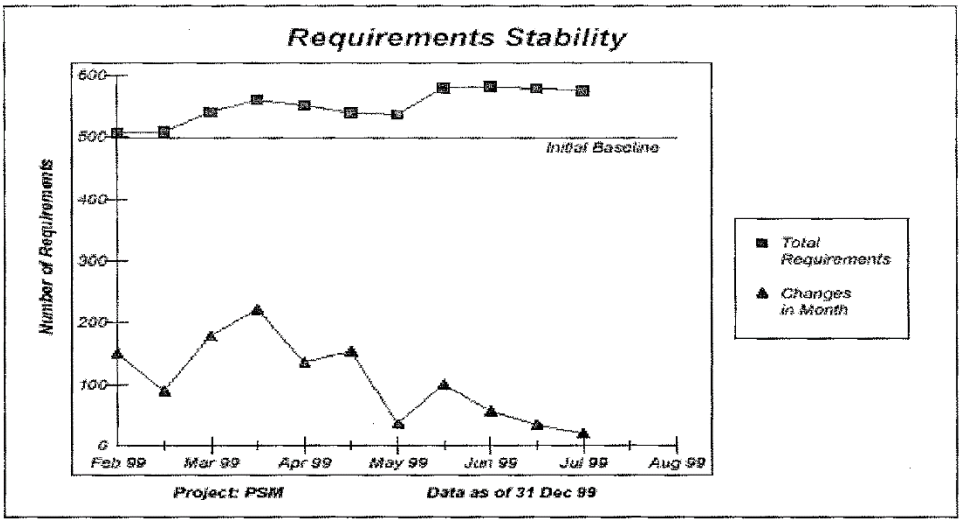


Figure Q–6. Requirements stability—total requirements versus changes

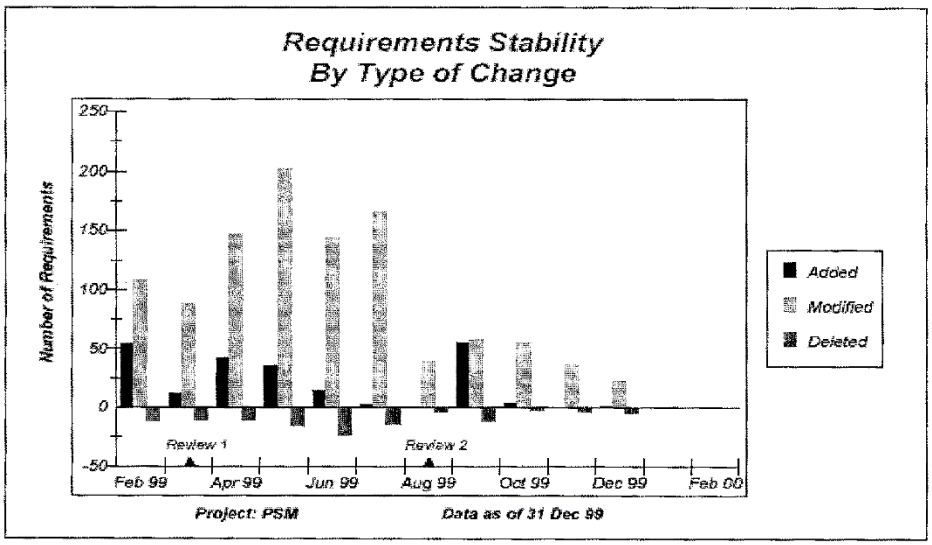


Figure Q–7. Requirements stability—type of change

Table Q–12
Software metric—design stability common issue—product size and stability

Selection guidance	Specification guidance
Project application - Begin tracking as design modules are approved and entered into configuration management and continue for each version until completion.	**Typical data items** - Date planned for design/delivery increment completion. - M = Number of units in current delivery/design. - Fc = Number of units in current delivery/design that include

Table Q–12
Software metric—design stability common issue—product size and stability—Continued

Process integration - Easier to collect if formal reviews, inspections, or walkthroughs are included in the development process. - Data are usually available from the configuration management system in a mature and disciplined development process. **Usually applied during** - Requirements analysis (Estimates). - Design (Estimates and Actuals). - Implementation (Estimates and Actuals). - Integration and test (Estimates and Actuals). - Operations and maintenance (Estimates and Actuals).	design related changes from previous delivery. - Fa = Number of units in current delivery/design that are additions to previous delivery. - Fd = Number of units in previous delivery/design that have been deleted. - T = Total number of units projected for system. **Typical attributes** - Product or identifier. - Increment. - Technology source (COTS, Government-off-the-shelf, NDI, reuse). **Typical aggregation structure** - Software increment or release. **Typically collected for each** - CI or equivalent. - Software increment or release. **Count actuals based on** - Each new release or revision of a product or process that implements changes.

(b) Management information.

1. The design stability measure depicts how much of a software delivery, or version, is comprised of pieces reused without modification from the previous delivery or version. The closer this value is to one, the higher the amount of reuse.

2. The design stability measure should be monitored to determine the number and potential impact of design changes, additions, and deletions on the software configuration. The trend of the measure over time indicates the software design is approaching a stable state when the curve levels off at a value approaching one.

3. The higher the design stability measure, the better the chances of a stable software configuration. However, a value close to one is not necessarily good unless M is close to the total number of units required in the system (design progress measure approaching one), and the number of changes being counted is relatively small and diminishing over time. Periods of inactivity could be mistaken for stability.

4. When design changes are being made to the software, the impact on previously completed testing must be assessed. Tests may need to be redone and may require modifications to test data and conditions.

5. Allowance for exceptional behavior of this metric should be made for the use of rapid prototyping. Prototyping, while possibly causing lower design stability numbers early in the program, should reduce the number of design changes needed during later stages of development.

6. The PM should establish criteria to define what constitutes a "design change." A design change implies change to the code for specific reasons, not a change due to style or coding preferences or to add comments.

7. Be aware that this metric does not measure the extent or number of changes in a software unit or the quality of its code. Other metrics, such as complexity, can contribute to such an evaluation. This metric also does not identify the specific units that are being changed.

8. The design stability metric can be used in conjunction with the complexity metric to highlight changes to the most complex units. It can also be used with the requirements metrics to highlight changes to units, which support the most critical user requirements.

9. If tracking design stability for builds or increments, T will likely be less than the total number of units projected for the system but will reflect the total projected for the build.

(c) Indicators.

1. Plotting the calculated design stability (S) and design progress (DP) values over time as in figure Q–8 is a recommended display. Directly below are the formulas for the two design measures. S = [M (Fa + Fc + Fd)] / M Where S = design stability measure. DP = M / T Where DP = design progress measure.

2. Although not indicated in figure Q–8, it is possible for design stability to be a negative value. This may indicate that everything previously delivered has been changed and more units have been added. If the current delivery contains fewer units than the previous one, a negative value indicates that the number of units deleted or changed from the previous baseline was greater than the total number of units in the current delivery.

3. If some units in the current delivery are to be deleted from the final delivery, it is possible for design progress to be greater than one.

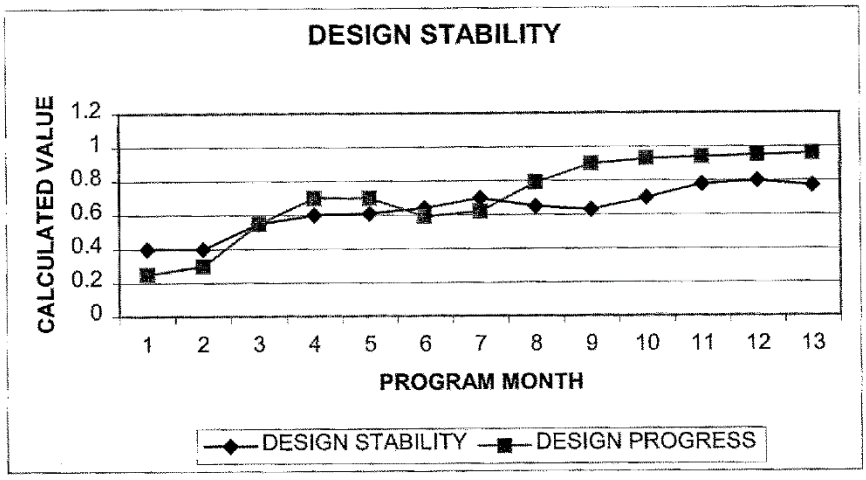


Figure Q–8. Design stability versus design progress graph

(6) *Complexity metric.*

(a) Army metric information. The cyclomatic complexity metric shown in table Q–13 counts the number of unique logical paths in a software component and can also evaluate the complexity of control or information flow in a system. This metric provides an indication of both design quality and the amount of testing required. Complexity measures provide a means to measure and evaluate the structure of software units. Software that is more complex is harder to understand, test adequately and maintain. Additionally, a highly complex unit is more likely to contain embedded errors than a unit of lower complexity. The likelihood of introducing errors when making code changes is higher in complex units. This metric answers such questions as—

1. How many complex components exist in the project?
2. What components are the most complex?
3. What components should be subject to additional testing or reviews?
4. What is the minimum number of test cases required to test the logical paths through the component?

Table Q–13
Software metric—complexity common issue—product quality

Selection guidance	Specification guidance
Project application - Begin collecting cyclomatic complexity during software design. - Recompute the complexity measures for units after they are modified during development and PDSS. - This metric should not be used unless the software developer has prior experience in measuring cyclomatic complexity. **Process integration** - Operational requirements may require efficient, highly complex code. - Measuring cyclomatic complexity requires a software	**Typical data items** - Programming language used for design. - The number of independent control paths through a unit, from entry point to exit point (also called basis paths). **Typical attributes** - Software unit. - Software increment or release. **Typical aggregation structure** - Software increment or release.

Table Q–13
Software metric—complexity common issue—product quality—Continued

developer to invest in specialized automated tools and defines a specific process for unit design approval. **Usually applied during** - Design (Actuals). - Implementation (Actuals). - Integration and test (Actuals). - Operations and maintenance (Actuals).	- Software component. **Typically collected for each** - Unit or equivalent. **Count actuals based on** - Passing inspection. - Passing component test. - Release to configuration management.

(b) Management information.

1. Automated tools are available for many programming languages and software development environments and should be used to assist in computing the complexity measures.

2. This metric applies throughout the software life cycle. Establishing a complexity threshold during development stimulates structured programming techniques and limits the number of critical paths in a program during design and unit implementation. Complexity is used during software testing to identify basis paths, define and prioritize the testing effort, and assess the completeness of unit testing. During PDSS, proposed changes that would substantially increase complexity should be examined closely, as they could also increase testing effort and decrease maintainability.

3. It is recommended that this metric be used to limit the inherent complexity of software during design and as code is being developed. Although the metric provides valuable information, it should not be relied upon as the sole metric to judge the quality of the design's implementation.

4. Complexity measures should be generated for each unit in the system. They can be grouped for display in a number of ways (for example, by CSCI, by individual unit, and so forth). Examining complexity at various levels can provide indications of potential problem areas. These indications give guidance to the developer on areas where additional concentration is needed. The Government can use complexity to find areas where test efforts should focus, such as performing code walk-throughs, more comprehensive unit level testing, or stress testing. While the majority of units can have values less than or equal to the criteria, it is possible that several units can have values exceeding 10. These units should be examined closely through testing and analysis.

5. In cases where units have a high cyclomatic complexity (many independent control paths), various techniques exist to help identify how complexity may be reduced. One method assesses the unit's actual complexity to identify control paths that cannot be tested. This can occur when a program's data flow and data conditions at various decision points preclude control from ever taking those paths. These sections are candidates for rewrite or elimination. Another method examines essential complexity, a gauge of the use of standard structured control constructs.

6. Units planned for reuse should not be overly complex.

7. Examining complexity trends over time can provide additional useful insights, especially when combined with other metrics such as design stability or development progress. For example, late software code "patches" may cause the complexity of the patched unit to exceed an acceptable limit, indicating that the design rather than the code should have been changed. Test resources may be better expended on units that have a relatively high structural complexity rather than on units that will reflect a high number of lines of code tested.

(c) Indicators.

1. The bar chart in figure Q–9 identifies the number of components in each complexity range. Each component within CI A was measured using an automated code complexity analysis tool. Component complexity values were separated into six complexity range categories and graphed. The threshold was also plotted. Figure Q–10 indicates that most CI A components are less than or equal to the maximum threshold of ten for component complexity.

2. Figure Q–10 was produced by sorting the components by complexity and showing only those components with a complexity higher than the threshold. CIs with a complexity higher than the threshold are candidates for redesign or additional review, inspection, and test.

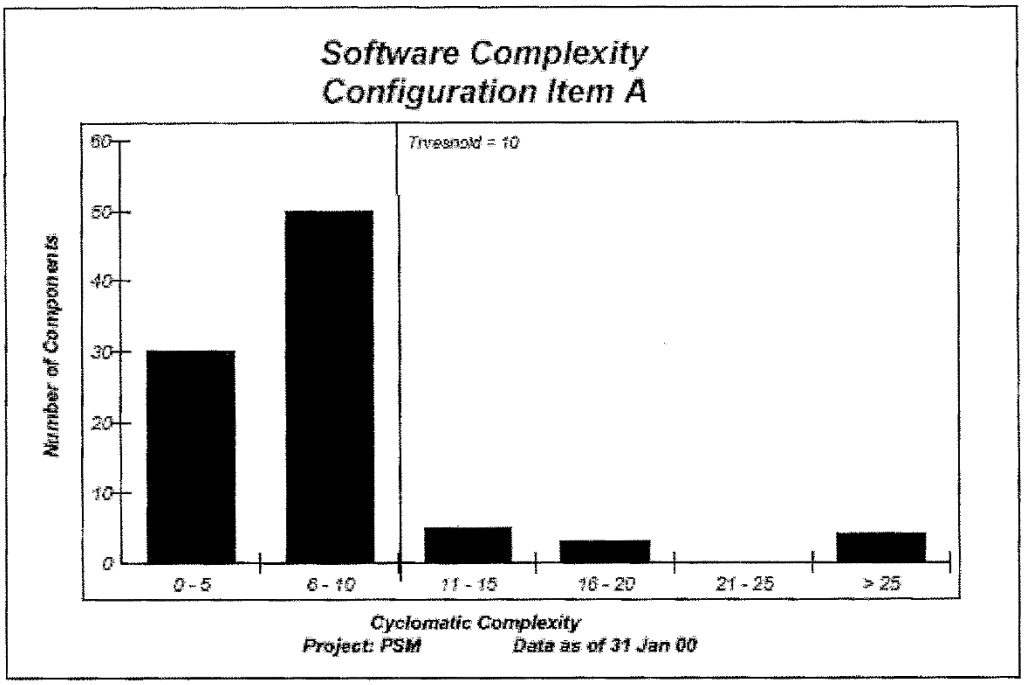


Figure Q–9. Software complexity—number of components

Software Complexity
For Configuration Item A
Units with Complexity > 10

Unit	Cyclomatic Complexity
A10	53
A2	49
A12	32
A11	27
A5	20
A9	19
A7	16
A8	15
A6	15
A1	13
A4	12
A3	11
A12	11

Project: PSM
Data as of 31 Jan 98

Figure Q–10. Software complexity—greater than threshold

(7) *Breadth of testing metric.*

(a) Army metric information. The breadth of testing metric at table Q–14 addresses the degree to which required functionality has been successfully demonstrated as well as the amount of testing that has been performed. This testing can be described as "black box" testing, since it is only concerned with obtaining correct outputs as a result of prescribed inputs. This measure answers questions such as—

1. Have all the requirements been allocated to hardware or software components?

2. Are the requirements being tested as scheduled?
3. Is implementation of the requirements behind or ahead of schedule?

Table Q–14
Software metric—breadth of testing common issue—schedule and progress

Selection guidance	Specification guidance
Project application - Data collection should begin when any formal software testing is performed. - Test cases must be developed to demonstrate specific functional requirements in assigned test events, and test results assessed before meaningful data can be collected. **Process integration** - Requires disciplined requirements traceability and testing processes for successful implementation. - Allocated requirements should be testable and mapped to test sequences. If an automated design tool is used, the data are more readily available. - Can be applied for each unique test sequence, such as CI, integration, system, and regression test, including "dry-runs." - Specific test criteria must be defined to determine if a requirement has been successfully tested.	**Typical data items** - Type of requirements tested and evaluated (such as SRS, interface requirements specification, UFD). - Total number of that type of requirement allocated to the CSCI. - Number of requirements tested with all planned test cases. - Number of requirements successfully demonstrated. - Test identification (for example, UAT, CSCI qualification testing, system qualification testing, DT, OT). - It is advised to track software requirements (SRS and interface requirements specification) tested and passed through higher test levels beyond software qualification tests. - This metric does not track the test progress of individual requirements. It is advised that the "number of requirements" data items be cumulative values across tests. **Typical attributes** - Increment. - Early in a project, the requirements baseline is limited to high-level specifications. Later in a project, the requirements baseline expands and measurement data is traceable to components and test cases. - Some functional requirements may not be testable until late in the testing process, and others may not be directly testable due to limitations in the test environment. - Type of requirement (user, system, component, and software). **Typical aggregation structure** - Function. - Requirements specification. **Typically collected for each** - Type of requirement (user, system, component, and software). - Specification reference. - Test sequence reference. **Count actuals based on** - Successful completion of all tests in the appropriate test sequence.

(b) Management information.

1. The breadth of testing metric measures the quantity of testing performed and achieved on documented requirements. While most requirements are usually functional, the metric also captures the results of performance, recovery, safety, security, adaptation, and any other requirements imposed by the acquirer that can be demonstrated through testing.

2. The overall success measure provides insight into the level of progress made toward implementing the approved requirements baseline.

3. Any change in the software requirements baseline requires recalculating the breadth of testing measures.

4. Data should be collected throughout developmental test activities, if possible. Typically, breadth of testing is collected for CSCI qualification testing and system-level tests.

5. The breadth of testing metric should also be reported incorporating the results of Government tests, such as DT and OT, particularly if there are requirements that cannot be adequately demonstrated prior to these system tests.

6. PMs should be aware of which software requirements cannot be tested until late in the testing process, or if a software function cannot be demonstrated at all prior to deployment.

7. An innovative option to assign a priority level to each user and software requirement to identify the most important requirements to be implemented in the software. Data for this metric may be collected and reported separately for each requirements priority level to provide more detailed visibility into which requirements are being tested.

8. As requirements are added and deleted over time, the population of total requirements also changes. This can cause the reported breadth of testing measures to fluctuate for reporting periods when no testing was performed.

9. When changes are made to requirements or design, previous test results for those areas are no longer valid. Until retesting and re-evaluation of results occurs, the number of requirements tested and number of requirements passed reported in breadth of testing should drop by the number of requirements to be retested.

10. Without clear criteria for test success, the breadth of testing metric may not be effective, due to the subjectivity in assessing whether a requirement has actually been satisfied.

(c) Indicators.

1. Figure Q–11 is a line graph of the number of successfully tested requirements. The graph reveals that testing is proceeding close to plan, with almost 80 percent of requirements tested to date.

2. The indicators in figure Q–12 can help quantify the expected product quality or the product's readiness to proceed to the next project phase. The top line shows the total number of interface requirements to be validated for the product. A second line shows the planned validation path for checking the interfaces. A third line represents the cumulative number of requirements successfully tested each week.

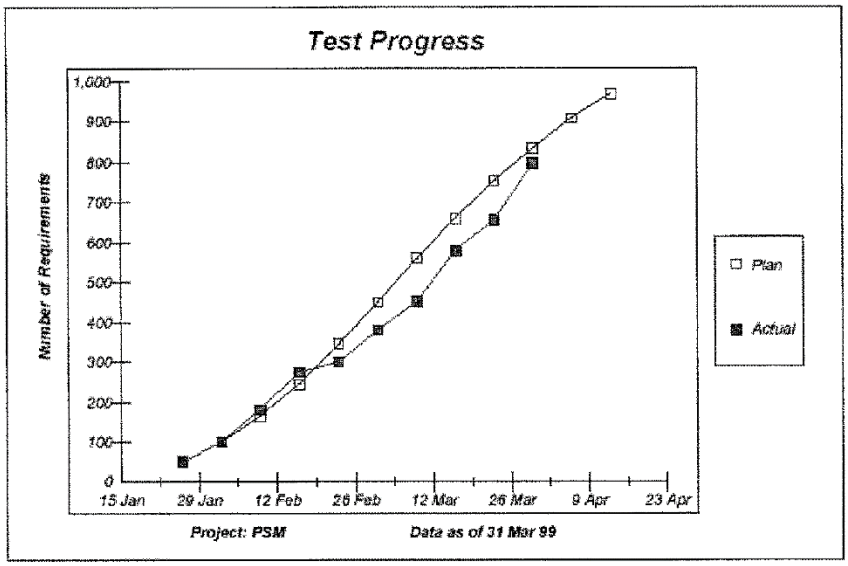


Figure Q–11. Number of requirements tested

(8) *Depth of testing metric.*

(a) Army metric information. The depth of testing metric shown in table Q–15 measures the amount of testing achieved on the software architecture, for example, the extent and success of testing as well as the possible control and data paths and conditions within the software. This testing is often described as "white box" testing, since there is visibility into how the software is constructed. This metric answers such questions as—

1. Is test progress sufficient to meet the schedule?
2. Is the planned rate of testing realistic?
3. What functions have been tested or are behind schedule?

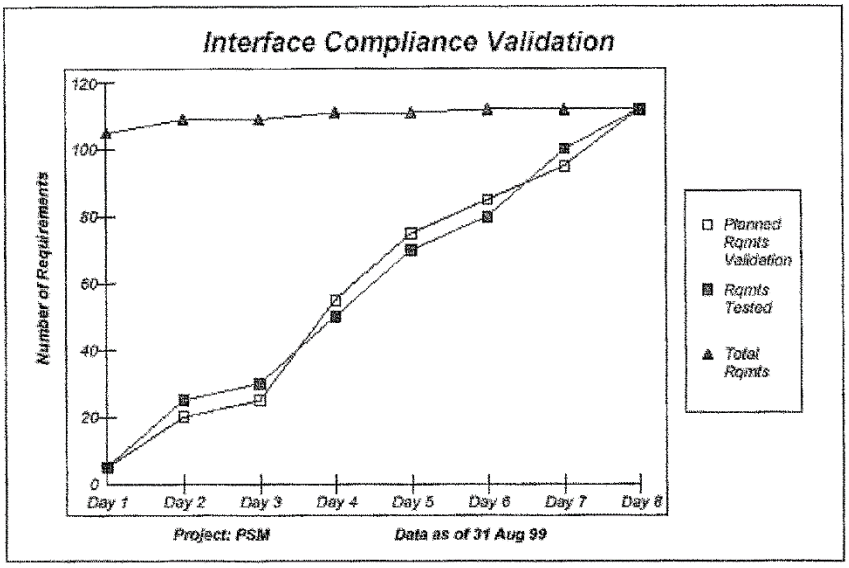


Figure Q–12. Requirements testing

Table Q–15
Software metric—depth of testing common issue—schedule and progress

Selection guidance	Specification guidance
Project application - Begin collecting data when a configuration controlled code baseline is available for unit testing. - Collect data in regression testing as changes occur in the baseline during development and PDSS. - The successful execution of path, statement, input, and decision point attributes of software structure can be monitored. - Specific test criteria must be defined before meaningful data can be gathered. - Each decision point which contains an "or" statement should be tested at least once for each of the condition's logical predicates. **Process integration** - Specialized test tools are needed to implement this measure successfully. - Can be applied for each unique test sequence, such as component, integration, system, and regression test, including "dry-runs." - Tests are performed at the unit level using design or architecture information. **Usually applied during** - Unit test (Estimates and Actuals). - Integration and test (Estimates and Actuals). - Operations and maintenance (Actuals).	**Typical data items** For each unit in each CSCI, collect— (1) Measured attribute (path or decision point). (2) Total number of attribute occurrences. (3) Number of occurrences executed at least once. (4) Number of occurrences successfully executed at least once. **Typical attributes** - Software increment or release. - Test sequence. - Test environment. - Test configuration. **Typical aggregation structure** - Software component. - Software increment or release. **Typically collected for each** - CI. **Count actuals based on** - Successful completion of each test case in the appropriate test sequence.

(b) Management information.

1. The depth of testing metric provides information on the integrity of the software design, including the relationship between the paths, statements, inputs, and decision points of the software.

2. The depth measures discussed here do not assess the "correctness" of design or code. It is expected that unit tests and unit integration and testing will make use of test cases that demonstrate code is designed properly. These cases should be supplemented by other cases to yield coverage and success measure that provides satisfactory confidence that unexpected control or data conditions will not occur. Software test programs usually require that software structure be successfully demonstrated only after passing some "realistic" number of test cases, under both representative and maximum stress loads. It is understood that fully exhaustive testing of all control and data combinations is prohibitive.

3. Because illegal inputs are used, the domain measure provides an indication of the robustness of the software design.

4. Some judgment is required to interpret the domain measure because it is unlikely that the program will be subjected to all possible input streams. However, the domain measure is important because most faults appear at domain boundaries.

(c) Indicators.

1. The attributes counts collected can be used to measure test coverage (the number of attribute occurrences tested and total number of occurrences of the attributes), and test success (number of attribute occurrences passed and total number of occurrences of the attributes).

2. Figure Q–13 is a line graph of the number of successfully tested requirements. The graph reveals that testing is proceeding close to plan, with almost 80 percent of requirements tested to date.

3. Figure Q–14 graphs the same components completing the next development activity, which is testing. Three progress measures are compared: the original plans for component test completion, components for which tests have been attempted, and components that have passed testing. Figure Q–14 indicates that not as many components have been tested as originally planned, and not all of the components that were tested passed. In fact, a large number of tests failed.

(9) *Fault profiles metric.*

(a) Army metric information. The fault profiles metric in table Q–16 shows a summary of software PCR data collected by the corrective action system. This metric provides insight into the number and type of deficiencies in the current software baseline, as well as the developer's ability to fix known faults. It answers questions such as—

1. What faults have been reported?
2. Have configuration managers approved the fault report?
3. Are the fault reports being closed at a sufficient rate to meet the test completion date?
4. Is the product maturing, that is, is the fault report discovery rate going down?
5. When will testing be complete?
6. What components have the most open fault reports?

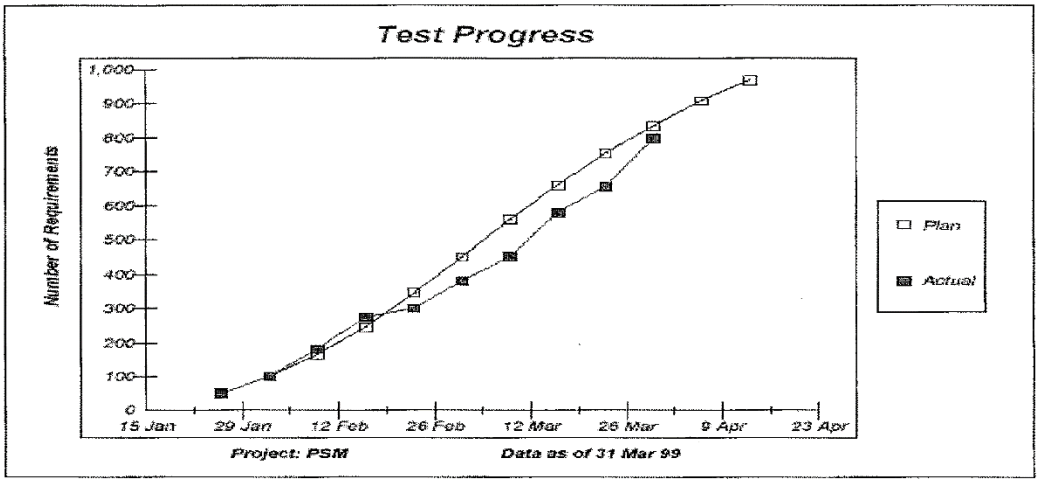


Figure Q–13. Progress

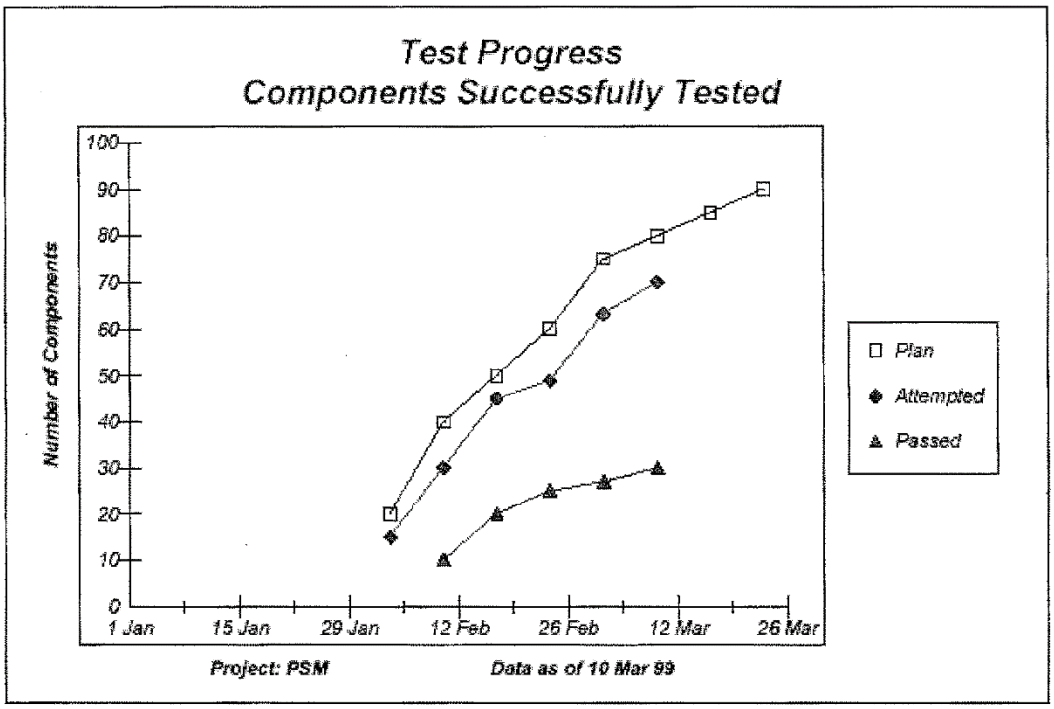


Figure Q–14. Components successfully tested

Table Q–16
Software metric—fault profiles and common issue—schedule and progress—Continued

Selection guidance	Specification guidance
Project application - Collection begins early in the software life cycle when the first software product, usually a requirements definition document, has been approved and placed under configuration control. - Continue to collect fault profiles data for the life of the program. - A corrective action system is the source of problem/change report, or fault, information for this metric. - To compute the age of faults, individual faults need to be tracked by the corrective action system, with the dates of problem start and problem closure recorded. **Process integration** - Requires a disciplined fault tracking process, including training of users, operators, and testers. Easier to collect if an automated system is used.	**Typical data items** - Cumulative number of faults detected. - Cumulative number of faults closed. - Average age of open faults. - Average age of closed faults, which is the same as average time to close. - Average age of all faults. **Typical attributes** - Software increment or release. - Fault priority. - Fault report status (open, closed). - Category (requirement, documentation, design, software, or other). - Phase of occurrence. - Valid/Invalid PCR. **Typical aggregation structure** - Component. **Typically collected for each** - CI or equivalent. - Test logs or operational incident reports. - The causes of faults may be reported, such as requirements specification problems, component design, operator error, or

Table Q–16
Software metric—fault profiles and common issue—schedule and progress—Continued

	documentation errors. - Some projects specify defect or reliability threshold limits, such as an acceptable number of PCRs or operational faults over time. - Operating time to fault may be based on component operating time or clock time. **Usually applied during** - Requirements Analysis (Estimates). - Design (Estimates and Actuals). - Implementation (Estimates and Actuals). - Integration and Test (Estimates and Actuals). - Operations and Maintenance (Actuals). **Count actuals based on** - Fault report recorded. - Fault report approved by configuration managers.

(b) Management information.

1. Fault counts should be based on all tests and evaluations on a formal baseline, which is under configuration control. Results of informal test-fix-test performed at the unit level should not be counted.

2. The gap between open and closed faults should be closely monitored. A constant gap or a continuing divergence is reason for the user representative to take appropriate action, especially when approaching a key test or milestone.

3. Inadequate problem resolution by the developer can cause the cumulative number of closed faults to remain constant over time, and a number of faults will remain open. The age of the open faults should be checked to see if they have been open for an unreasonable period of time. Those faults, which are not resolved, represent an increased risk. Managers should identify the reason that faults are not closed and take corrective action.

4. Managers should be aware of the cumulative effect of a large number of low priority faults. Too many minor problems may impair overall system operation or successful test conduct. PMs may wish to establish thresholds to limit the cumulative effects of unresolved priority 3 and lower faults on cost or ability to operate the system effectively.

5. The PM should establish a clear description of when a fault is considered discovered and closed. Criteria for the date discovered might be the date on which the original problem report was written, or when the report was entered into the corrective action system. Criteria for the date closed should reflect the CCB's judgment that regression testing was adequate and applicable documentation is updated. Differences in defining corrective action event dates can significantly influence the average ages reported via this metric.

6. Average age graphs can track whether the time to close faults is increasing over time. Increasing time to close faults may indicate that the developer is not allocating adequate resources to correcting problems, or that some faults are exceedingly difficult to fix.

7. Large deviations of individual faults from the average age of all faults should be investigated. The average open age of high-priority faults should also be examined with respect to the time remaining to the next major test or milestone.

8. Examining the categories of software faults can provide insight into the underlying problems. During the early stages of software development, the fault profiles metric reports the quality of translating software requirements into the design. Design faults suggest that requirements were not defined correctly, or that the developer is misunderstanding them. Later, the fault profiles metric measures the implementation of requirements and design into code, assuming an adequate level of testing is performed. Code faults could result from an inadequate design, or a poor job of implementing the design into code. Examining the fault categories to determine causal relationships should be performed in any analysis of fault profiles. Be aware that a single fault may be assigned to one or more categories.

9. The PM should understand any fault or "bug" tracking tools used by the developer for tracking fault profiles data. The developer's system for collecting problem reports should be reviewed early in the program to determine how much of a difference there is between the recommended data definitions above and the definitions used by the tool.

10. The PM should establish criteria to determine when a fix must be validated and by whom (Government or developer software quality assurance).

11. The PM should examine the following issues, which are not reported in the fault profiles data—

12. Time/cost of correction. The cost and time to correct a fault is not directly linked with the fault's priority. Priority 1 faults may be caused by trivial errors in syntax, while priority 4 faults may require a redesign.

13. Problem description/prioritization is not always obvious. For example, a single character error in a source statement which leads to an improperly executed function. Interpretations of problem and priority may be different depending on whether the cause or effect is emphasized. The method for determining fault categories and defining fault priorities is not as important as applying the definitions consistently.

14. Category of fault. Faults in requirements are often the most expensive and persist the longest. These faults may not be detected until the software is used on site. Design faults could be related to processing or control flow. If these faults persist past unit-level testing, check inputs tested as reported in the breadth of testing metric. Control and sequence faults in code may include missing paths, unreadable code, loop termination criteria incorrect, uncontrolled GOTOs, and spaghetti code (old COBOL). These faults are often caught with path testing. If many of these types of faults persist beyond unit testing, check the depth of testing metric for completeness.

15. The fault profiles displays do not identify which individual faults persist over time. The developer's corrective action system may identify the software unit related to a fault to indicate product status. With unit identifiers, it may be possible to identify problem units and combine analysis with other metrics for a more complete diagnosis.

16. When interpreting fault profiles data, be aware that error detection is closely tied to the quality of the development and testing process. A low number of detected faults could indicate either good process management with good products, or a process with an inadequate amount or improper type of testing. Fault profiles metric data should not be evaluated without also considering measures of test coverage. For example, a plot of code category faults could be evaluated against the amount of testing which was done in each month. The relationship of code faults to test coverage can be used to gauge the maturity of software and the adequacy of the test program.

17. Reliability models can be used to forecast the rate additional faults will be discovered based on previous error detection history.

(c) Indicators.

1. A line chart (see fig Q–15) shows both the cumulative number of problem (fault) reports and the number of fault reports closed to date. The difference represents the total number of problem reports that are still open. Figure Q–15 indicates that a large number of new faults have been discovered over the past year. However, in the past several months, the reporting rate has tapered off. While the closure rate has not kept pace with the reporting rate, the number of open fault reports is shrinking, as faults are steadily being closed, and fewer new ones are being reported.

2. To learn more about the remaining open problem (fault) reports, additional analyses were performed. The bar chart in figure Q–16 includes all open fault reports divided into categories by age. This was done by calculating the number of days elapsed since the fault was reported and grouping the fault reports by age. Figure Q–16 shows an average open age of 5.7 weeks. This average is below the desired maximum of 8 weeks. The maximum age of faults is determined by considering the length of the project, the project's current status, delivery requirements, and the type and severity of defects discovered.

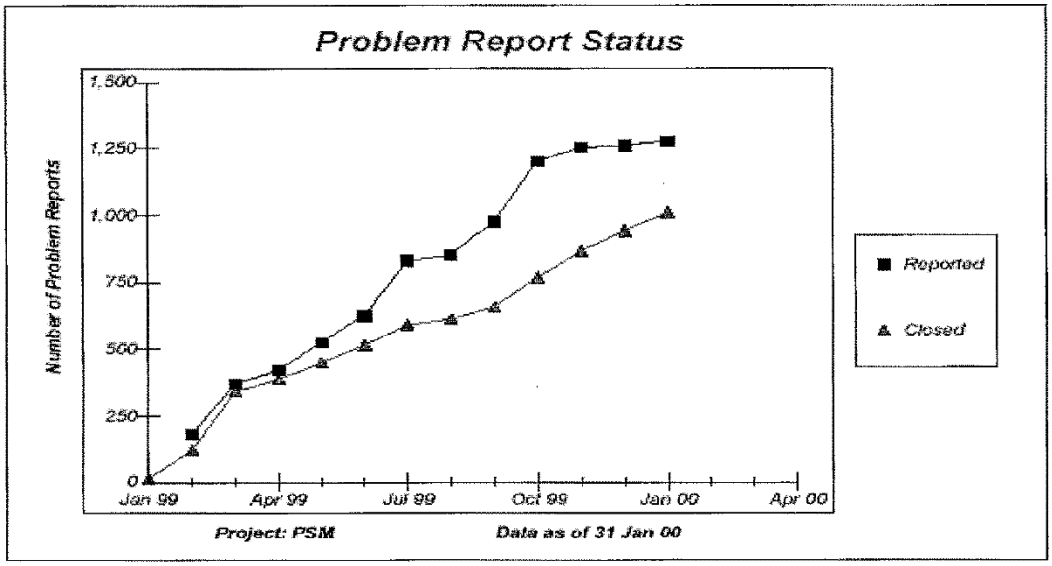


Figure Q–15. Fault status

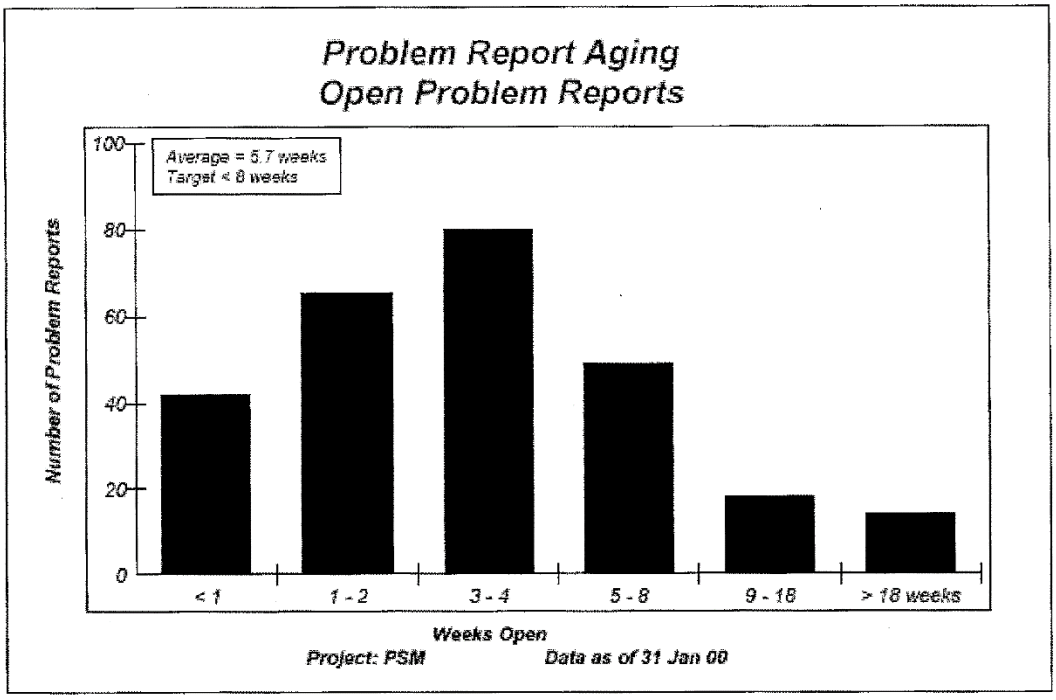


Figure Q–16. Fault aging

(10) *Reliability metric.*

(a) Army metric information. The reliability metric shown in table Q–17 measures the ability of software to perform as intended. The software contribution to system mission reliability is measured by the number of system failures caused by software and the time it takes to restore the system to its previous operating condition. Another measure

can be used to track defect data obtained from PCRs during software development and use analytic models to predict operational reliability. Using data from the fault profiles metric and test history can project future failures as a function of test time (such as time to next failure or failure rate) and to project the number of latent, or as yet unobserved, faults remaining in a software baseline. These projections can be used to gauge how much testing is required for confidence that critical faults will be within acceptable limits when the software is fielded. This metric answers questions such as—

1. What is the system's operational reliability?
2. Is the system ready for operation?
3. How often (and how severely) will the system/component fail during operation of the system?
4. Will the system, component, or function be available for use when it is needed?

(b) Management information.

1. Fault counts should be based on all tests and evaluations on a formal baseline, which is under configuration control. Results of informal test-fix-test performed at the unit level should not be counted.

2. The gap between open and closed faults should be closely monitored. A constant gap or a continuing divergence is reason for the user representative to take appropriate action, especially when approaching a key test or milestone.

3. Inadequate problem resolution by the developer can cause the cumulative number of closed faults to remain constant over time, and a number of faults will remain open. The age of the open faults should be checked to see if they have been open for an unreasonable period of time. Those faults, which are not resolved, represent an increased risk. Managers should identify the reason that faults are not closed and take corrective action.

4. Managers should be aware of the cumulative effect of a large number of low priority faults. Too many minor problems may impair overall system operation or successful test conduct. PMs may wish to establish thresholds to limit the cumulative effects of unresolved priority 3 and lower faults on cost or ability to operate the system effectively.

5. Managers should establish a clear description of when a fault is considered discovered and closed. Criteria for the date discovered might be the date on which the original problem report was written, or when the report was entered into the corrective action system. Criteria for the date closed should reflect the CCB's judgment that regression testing was adequate and applicable documentation is updated. Differences in defining corrective action event dates can significantly influence the average ages reported via this metric.

6. Average age graphs can track whether the time to close faults is increasing over time. Increasing time to close faults may indicate that the developer is not allocating adequate resources to correcting problems, or that some faults are exceedingly difficult to fix.

7. Large deviations of individual faults from the average age of all faults should be investigated. The average open age of high-priority faults should also be examined with respect to the time remaining to the next major test or milestone.

8. Reliability models can be used to forecast the rate additional faults will be discovered based on previous error detection history.

Table Q–17
Software metric—reliability common issue—product quality

Selection guidance	Specification guidance
Project application - Collect measures of system failures caused by software during formal system-level tests and continue through PDSS. - Collect reliability data only under typical system operating conditions. - Deriving a predicted software failure rate and estimating latent software faults requires an appropriate software reliability model. **Process integration** - Requires a disciplined failure tracking process, including training of users, operators, and testers. - It may be useful to categorize failure causes, including failures caused by requirements specification problems, component design, operator error, or documentation errors. - Some projects specify reliability threshold limits, such as an acceptable number of failures over time.	**Typical data items** - Test identification. - Achieved mean-time-between-failure (MTBF). - Mean, median, and maximum 95th percentile mean time to restore system to operational status. - Software reliability model used and test identification. **Typical attributes** - Failure identifier. - Type of failure. - Severity of failure effect. - Root cause of failure. - Phase of occurrence. - Corrective and preventive actions required. - Test sequence. **Typical aggregation structure**

Table Q–17
Software metric—reliability common issue—product quality—Continued

- The test environment must be representative of the operational environment and time to failure is based on system operating time. **Usually applied during** - Design (Estimates). - Implementation (Estimates). - Integration and test (Estimates). - Operations and maintenance (Actuals).	- Software component. - Software increment or release. **Typically collected for each** - Function. - CI or equivalent. **Count actuals based on** - Failure documented. - Failure validated. - Failure resolved.

(c) Indicators.

1. The MTBF indicator is often used to provide insight into system or software failure trends. This indicator shows the average time from one failure to the next, in operations or test. MTBF is often a system performance requirement, tracked as a technical performance measure.

2. After the desired MTBF requirement is established, it should be checked for feasibility against the system or software application and tracked to monitor performance against plan.

3. During planning and requirements analysis, assess the feasibility of meeting stated reliability requirements. Compare reliability requirements against historical performance data from similar systems. If the requirements are too stringent for the system type, it may be difficult to achieve the required MTBF, or it may not be a cost-effective design. However, if the requirement is lower than the range historically achieved, then operational performance may be in jeopardy.

4. Figure Q–17 graphs ranges of historical data for each system application, to help build reliability plans and to perform an MTBF feasibility analysis.

5. Figure Q–18 is an example of a reliability growth plan and the tracking of actual MTBF performance against the plan. In this example, the project was performing well against the plan during the first 2 months. However, the trend changed in March as reliability growth fell below the target value. A single month's performance was not enough to initiate major actions beyond understanding the causes of the change. When the variance from plan increased in April, the project identified the root causes of the problem and took corrective actions to improve performance. This intermediate tracking of MTBF helped to identify the growing risk of not meeting the required MTBF and to determine whether the corrective actions were working.

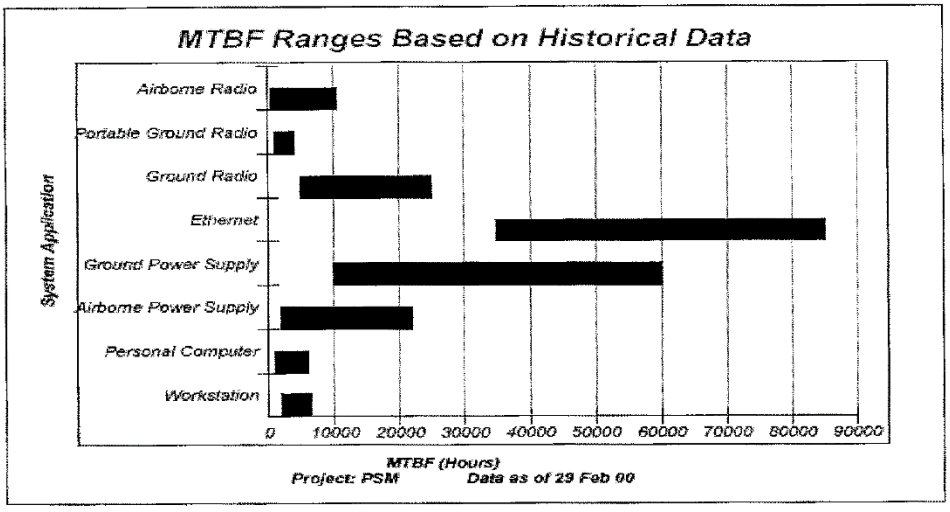


Figure Q–17. Mean-time-between-failure ranges

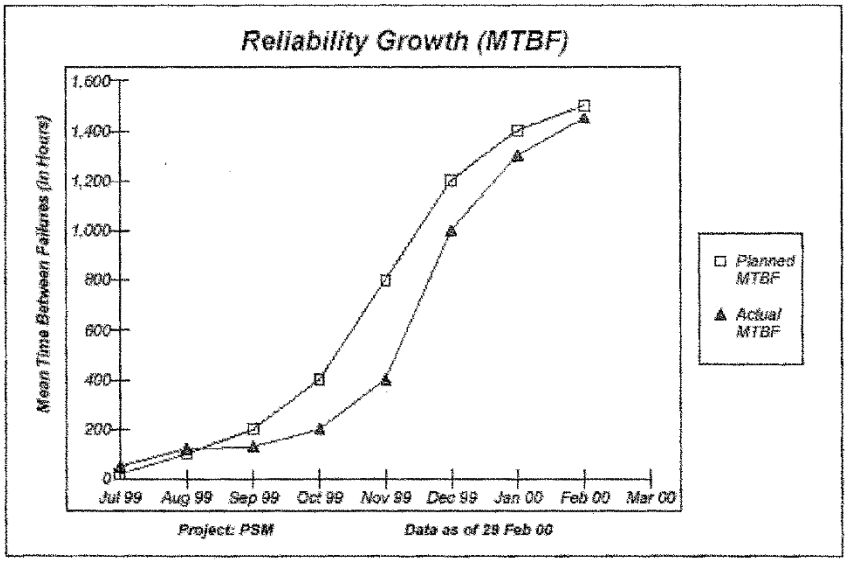


Figure Q–18. Reliability growth

(11) *Manpower metric.*

(a) Army metric information. The manpower metric shown in table Q–18 provides an indication of the developer's human-resource capability and ability to provide sufficient staffing to complete the project within the allotted the time and budget. The example manpower metric can be measured at two levels. A basic measure reports total labor hours planned and expended. A more detailed measure describes the number of personnel in various levels of qualifications and experience. This metric answers questions such as—

1. Are labor hours being applied according to plan?
2. Are certain tasks or activities taking more or less effort than expected?
3. Are sufficient experienced personnel available?
4. How many people have been added or have left the project?
5. What is the impact of personnel turnover rates?

Table Q–18
Software metric—manpower common issue—schedule and progress

Selection guidance	Specification guidance
Project application - This metric is applicable to all software development and maintenance projects and can be tracked for entire software life cycle. **Process integration** - Data are usually derived from the labor and financial accounting and reporting systems. - This metric should report all labor hours, including overtime, even if it is not compensated. - This measure is most effective when financial accounting and reporting systems are directly tied to individual products and activities at a WBS element level. - Counting personnel may be difficult if they are not allocated to the project on a full-time basis or if they are assigned to more than one WBS element.	**Typical data items** - Labor category. - Experience level. - Planned and actual number of labor hours expended in the reporting period. - Planned and actual number of personnel in a specific experience level for the reporting period. - Number of unplanned losses of personnel. **Typical attributes** - Organization. - Labor category. - Education level. - Experience factor. **Typical aggregation structure** - Project. - Organizational component.

Table Q–18
Software metric—manpower common issue—schedule and progress—Continued

	Typically collected for each - Project. - If labor hours are considered proprietary data and are not explicitly reported, data may be approximated from staffing or cost data. - Manpower planning data are usually based on estimation models, historical data, or engineering judgment. - Detailed data reporting requires a personnel database that includes experience and training data. - Detailed experience levels may be based on education, software language, system domain, or length of time together as a team. - Planned and unplanned personnel losses may be reported. **Usually applied during** - Project Planning (Estimates) and all other phases (Estimates and Actuals). - WBS Component. **Count actuals based on** - Financial or labor reports.

(b) Management information.

1. Software staff includes those engineering and management personnel directly involved with any software activity.

2. Losses and gains for each labor category should be tracked to indicate potential problem areas. High turnover of key and experienced personnel can adversely affect project success. Adding many unplanned personnel late in the development process may indicate impending problems.

3. Significant deviations from planned staffing levels may indicate problems in the developer's management procedures or problems in product quality that require additional effort to repair.

4. The shape of the staffing profile curve tends to start at a moderate level at the beginning of a project, grow through design, peak at implementation and testing and diminish near the completion of integration testing. Individual labor categories, however, are likely to peak at different points in the life cycle. Any significant deviation between actual and planned values should be investigated to determine the cause. During PDSS, staffing is usually constant.

5. The manpower metric is used primarily for project management and may not necessarily have a direct relationship with other technical and maturity metrics. For example, growth in number of personnel is not necessarily reflected by an increase in product quality.

(c) Indicators.

1. In figure Q–19, the latest plan (plan 2) is compared to the original plan (plan 1) and to the actual effort expended to date. While plan 2 appears more realistic (because it is more consistent with actual effort allocation to date), the acceptability of extending the schedule by several months must be determined. Also consider whether the new plan calls for additional effort overall. In this example, total effort has not increased; otherwise, the impact on project costs and the availability of additional resources should be considered.

2. Figure Q–20 tracks effort on a maintenance project with a fixed staffing level (level-of-effort project). While the fixed staffing level was incorporated into project plans, actual effort expended to date did not achieve this level. In March and April, several members of the project were loaned to another project. In May, some new persons were assigned to maintenance as a training opportunity. Due to summer vacations, less time was spent in July than planned.

3. Figure Q–21 shows that the supplier started the project with a staff average of 3.4 years of real-time distributed systems experience. To further investigate recent schedule slippage and low productivity, updated staff experience data was requested. The new data reveal that, while staff size has remained constant (in spite of turnover), the experience levels of replacement staff have dropped. The average experience is now only 2.4 years.

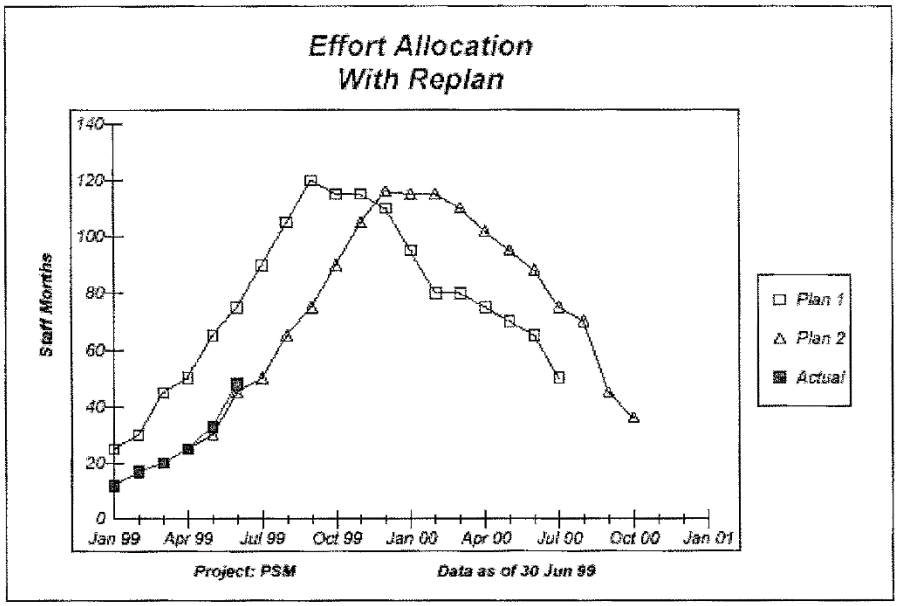


Figure Q–19. Level of effort (plans vs actual)

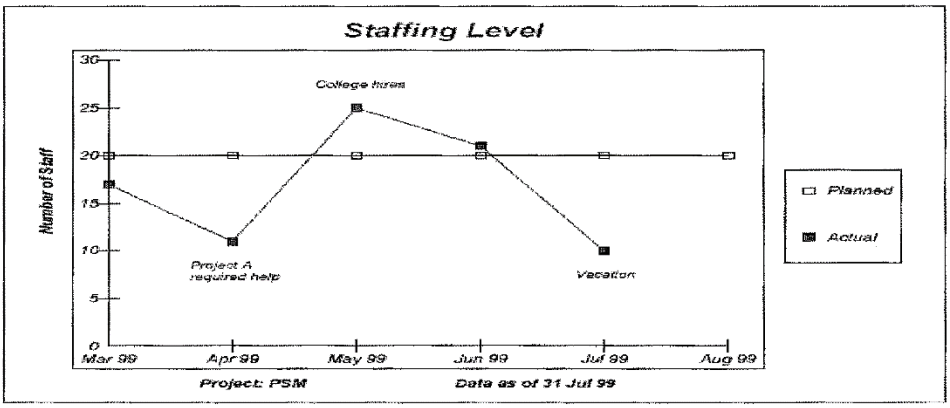


Figure Q–20. Staffing level planned vs actual

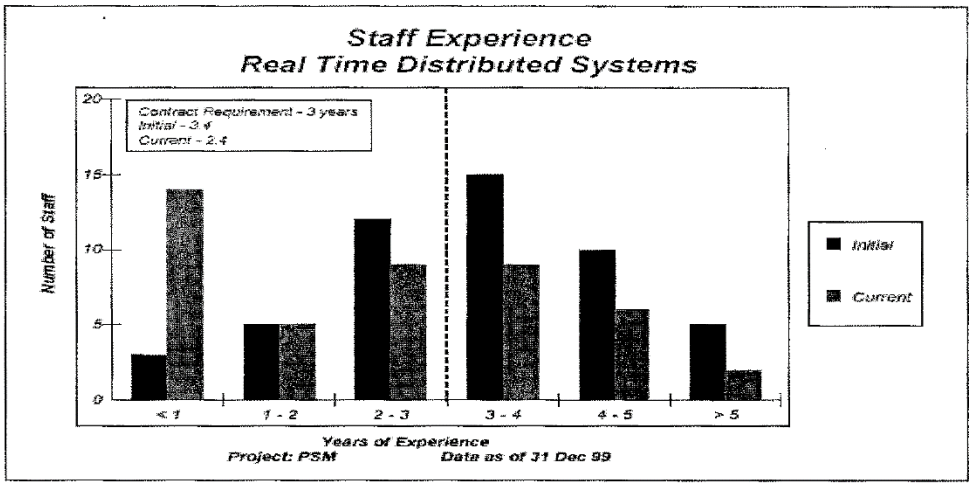


Figure Q–21. Staff experience

(12) *Development progress metric.*

(a) Army metric information. The development progress metric shown in table Q–19 measures the completeness of the software development or maintenance effort, based on the number of planned units of labor or product that are completed on a schedule. This metric answers questions such as—

1. Are components completing development activities as scheduled?
2. Is the planned rate of work activity realistic?
3. What components or work activities are behind schedule?

Table Q–19
Software metric—development progress common issue—schedule and progress

Selection guidance	Specification guidance
Project application - Data can be reported for this metric if the project has a disciplined process that can identify specific units of labor or products that are to be completed on a defined schedule. **Process integration** - Work units may include formal reviews, inspections, or walkthroughs in a development process. - Data are usually available from the configuration management or schedule processes. - Specific criteria must be established to define completion of a unit. **Usually applied during** - Begin collecting estimates during project planning and continue reporting estimates and actuals through operations and maintenance.	**Typical data items** - Number of software units in a software increment or release. - Planned and actual number of units completed. - **Typical attributes** - Software increment or release. - Type of activity or process. **Typical aggregation structure** - Software increment or release. **Typically collected for each** - CI or equivalent. - Software increment or release. **Count actuals based on** - Successful completion of a work phase. - Approval of a unit by configuration management.

(b) Management information.

1. Units of labor or products may be defined for all phase of software development and maintenance; including requirements definition, software design, code implementation and unit test, unit integration and test, and planned maintenance updates.

2. Examining the planned versus actual number of units completed may indicate potential problems with schedule and cost.

3. The number of units completed may not indicate product quality and rework that may be required.

4. Other example metrics related to development progress are cost, schedule, computer resource utilization (CRU), requirements traceability, requirements stability, and complexity.

(c) Indicators. Figure Q–22, design progress, is graphed with a line chart depicting cumulative measures for the original plan (plan 1), the current plan (plan 2), and the actual components designed to date. Each point is calculated by adding the number of components allocated for the reporting period to the corresponding cumulative total from the last reporting period. The figure shows that design progress was behind the original plan at the end of August 1999, resulting in a new plan of the overall activity. Actual design progress has remained fairly close to the new plan (plan 2). The plan line, however, requires a significant increase in the completion rate over the next few months, raising concern about the feasibility of the plan.

(13) *Schedule metric.*

(a) Army metric information. The schedule metric shown in table Q–20 reports the planned and actual dates for completion of activities and products. Comparison of plans and actual completion of tasks indicated the level of risk in achieving future project goals. This metric answers questions such as—

1. Is the current schedule realistic?
2. How many activities are concurrently scheduled?
3. How often has the schedule changed?
4. What is the projected completion date for the project?
5. What activities, events, or products are on time, ahead of schedule, or behind schedule?
6. Will the target budget be achieved or will there be an overrun or surplus?

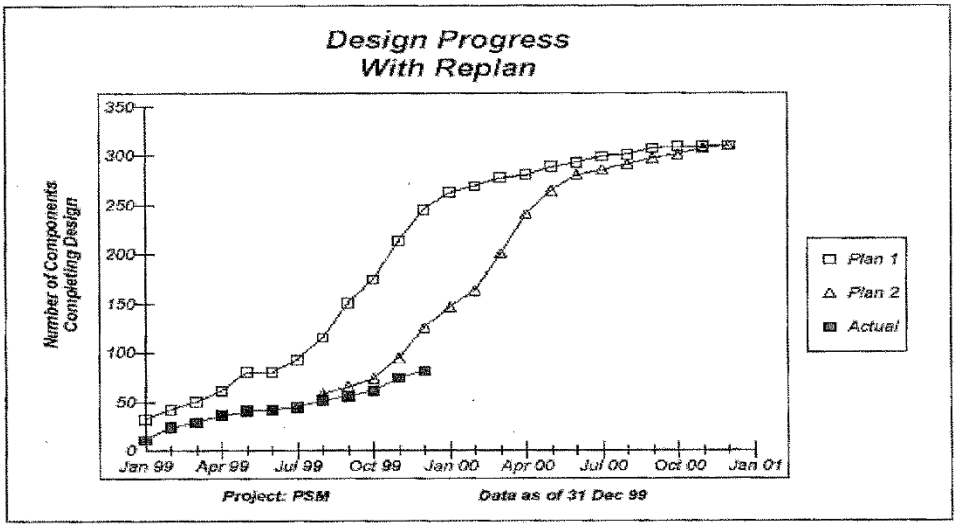


Figure Q–22. Design progress

Table Q–20
Software metric—schedule common issue—schedule and progress

Selection guidance	Specification guidance
Project application - Schedule data are reported in almost every Government and industry project. **Process integration** - The ability of a project to stay on schedule is determined by	**Typical data items** - Planned start date of activity or event. - Actual start date of activity or event. - Planned end date of activity or event. - Actual end date of activity or event.

Table Q–20
Software metric—schedule common issue—schedule and progress—Continued

the quality of the process to estimate and plan the original schedule. - Schedule data should be focused on major activities that will affect the critical path performance or high-risk activities. - If schedule dependency data are collected, slips in related activities can be projected and monitored. - If activities or events are re-planned to occur at a different time, the original dates should be retained in the schedule reports to indicate areas of risk.	**Typical attributes** - Activity. - Project. - Version, activity or event. - Product. - Version of the plan. - Software increment or release. - Organization. **Typical aggregation structure** - Component. - Activity. - Project. **Typically collected for each** - Activity. Some software maintenance projects are considered level-of-effort tasks and may not have detailed milestones; reporting only the dates of increment releases and change request closure. **Usually applied during** - Begin schedule estimating during project planning and continue reporting estimates and actuals through operations and maintenance. - Project or WBS element. - CI or equivalent. - Key activity. **Count actuals based on** - Successful completion of tasks. - Customer sign-off. - Project element complete (to defined exit criteria). - Product delivery.

(b) Management information.

1. During project planning and replanning, schedules should be analyzed to determine if any important activities or events are missing, if overlap between activities is feasible, and if dates and activity durations are reasonable, based on other project assumptions of the cost, staffing, and task difficulty.

2. When the schedule plan is changed, schedule slippage over time should be made apparent by retaining and reporting each successive plan in the schedule indicator.

(c) Indicators.

1. In figure Q–23, implementation ends slightly earlier in plan 4 than in plan 3, but integration and test finishes more than 1 month later in plan 4 than in plan 3. Given the extent of slippage that has already occurred on the project, the feasibility of meeting this new milestone must be evaluated. Throughout a project's life cycle, a Gantt chart may be used to help identify the current status of major project events and to assess the impact of actual schedule slips on future activities and milestones.

2. In figure Q–24, planned and actual start and end dates show the status of the last four maintenance releases. The first three releases were completed, while release 4 is still in progress. Both releases 1 and 2 were completed late, and release 4 is also projected with a late completion. For maintenance releases, late requirements changes often impact schedule and should be investigated.

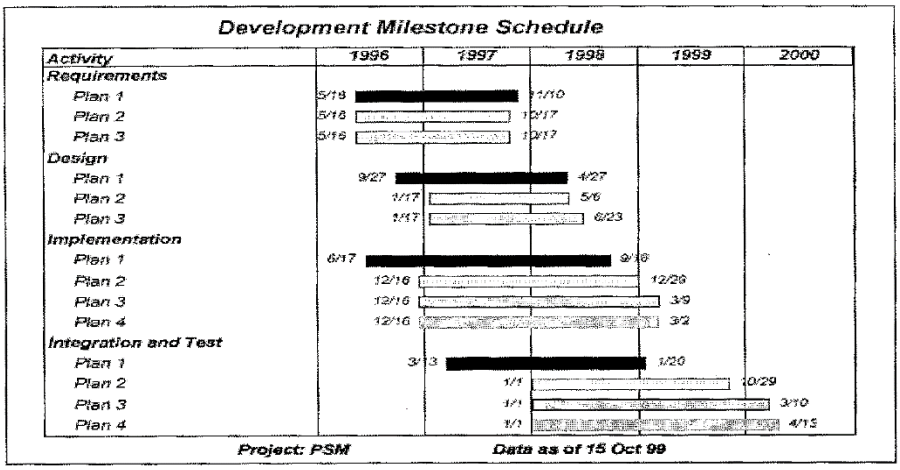


Figure Q–23. Development milestone schedule

(14) *Computer resource utilization metric.*

(a) Army metric information. The CRU metric shown in table Q–21 measures the planned and actual capacity of a component resource that is used during system operation. Component resources that are commonly monitored are computer processor utilization, input/output capacity, memory, and storage space use. The metric indicates whether the hardware capacity can support the software and system operational requirements. This metric answers questions such as—

1. Can additional data traffic be accommodated after system delivery?
2. Do estimates for the resource appear reasonable? Have large increases occurred?
3. Does hardware design have the reserve capacity to ensure software operation for all system functions?

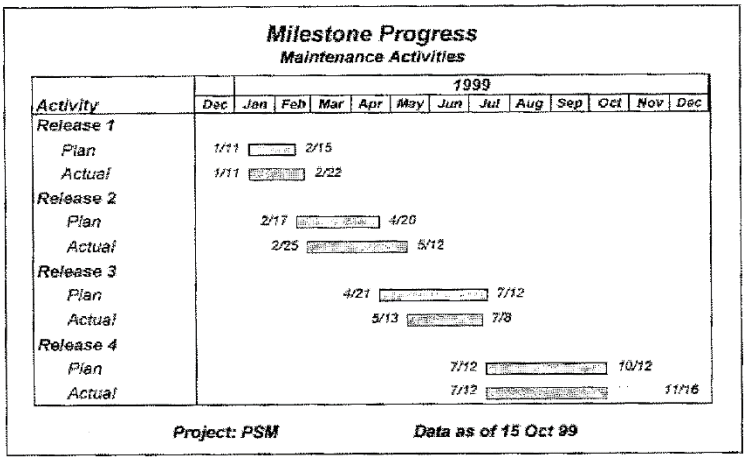


Figure Q–24. Milestone progress

Table Q–21
Software metric—computer resource utilization common issue—product quality—Continued

Selection guidance	Specification guidance
Project application - Critical for safety and high-reliability applications. - An important metric for resource-constrained systems. **Process integration** - The system must have a well-defined operational profile to allow accurate estimates of capacity utilization. - CRU estimates are difficult to derive and require significant simulation or modeling support. Estimates must be developed early to impact design decisions. - Actual measurement of CRU cannot happen until late in software development when operational software and realistic equipment are available. - CRU estimates should be based on the worst-case loading or stress that may occur in the defined operational profile.	**Typical data items** - Planned computer processor utilization. - Actual computer processor utilization and the measured impact on throughput and timing. - Planned and actual utilization of any measures resource (memory, storage, input/output, and network utilization). **Typical attributes** - Software increment or release. - Operational profile. - Hardware version. - Activity. - Project. **Typical aggregation structure** - Software increment or release. - Hardware component. **Typically collected for each** - Activity. - Project or WBS element. - CI or equivalent. - System resources may be insufficient even though individual component resources are adequate. **Usually applied during** - Project Planning (Estimates). - Requirements Analysis (Estimates). - Design (Estimates). - Implementation (Estimates). - Integration and Test (Estimates and Actuals). - Operations and Maintenance (Estimates and Actuals). - Software increment or release. **Count actuals based on** - Integrated system test. - Operational test and field reports. - Project element complete (to defined exit criteria). - Product delivery.

(b) Management information.

1. A recommended CRU reporting frequency does not exist and should be determined by the criticality of reserve capacity for a computer resource.

2. Resource capacity monitors are often designed as a part of the regular operating system functions.

3. Resource capacity estimation is difficult for hardware designs that employ dynamic allocation, virtual memory, parallel processing, multitasking, or multi-user features.

4. CRU can also be used to determine whether sufficient capacity exists to support operations under conditions of high usage or stress or if new functionality can be supported.

(c) Indicators.

1. Figure Q–25 shows the central processing unit (CPU) utilization of the system, measured against the contract requirement for a 50 percent reserve. This is based on a peak measurement. Both reliability and CPU utilization are based on a user-defined operational scenario. This figure indicates that tests show current utilization levels slightly above the 50 percent threshold.

2. A comparative evaluation of these four indicators reveals that the project is making steady progress in completing testing activities; that no large unplanned activities exist (as a result of rework); and that critical performance measures will probably be met. As a result, the team may proceed with plans to deliver the system as scheduled.

3. The remaining open problem reports should be reviewed to ensure that deferment of those problems will not adversely affect usability or key customer requirements. Any high-priority problems should be corrected prior to delivery.

4. Reducing the CPU utilization would probably require additional changes to some components that have otherwise been certified as working properly. This rework decision could delay delivery. The PM and customer may decide to make a tradeoff by accepting a system that exceeds the desired threshold to allow on-time delivery. A future enhancement might address the threshold problem.

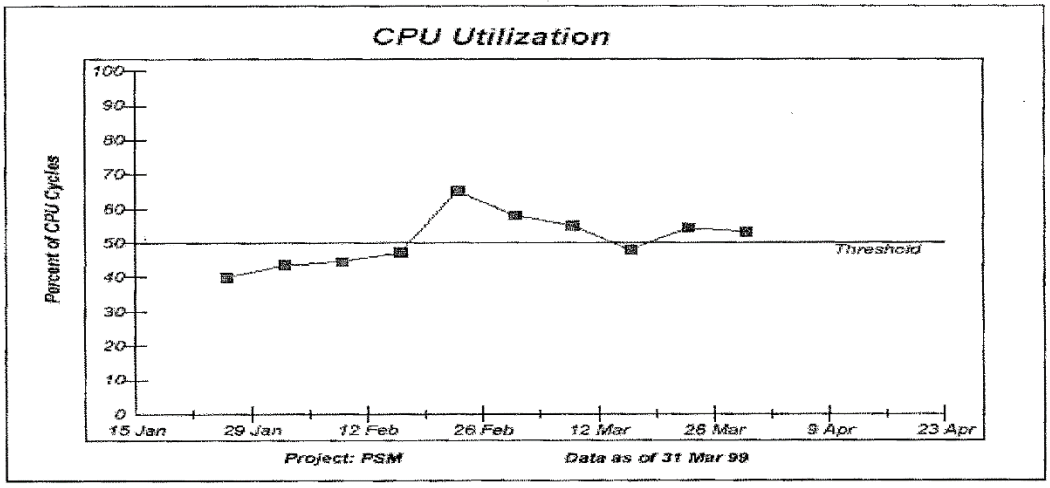


Figure Q–25. Central processing unit utilization

Section VII

Risk Assessment

Q–50. Risk and test and evaluation

a. T&E is expensive, carrying up to 50 percent of the development budget for large-scale systems, especially when they are software intensive systems. T&E events that cannot be completed due to inadequate preparation, safety hazards, or test failures may need to be repeated, wasting money and jeopardizing a program's chances of success. This appendix describes a structured method of evaluating risk associated with an upcoming T&E event. Assessing and mitigating risk is an important task for both the tester and the evaluator.

b. Risk is generally defined as exposure to potential adverse effects. In order to make an objective decision concerning T&E risk, it's necessary to—

(1) Identify the T&E event objectives.
(2) Identify risks that inhibit achieving these objectives.
(3) Assess the probability of each risk.
(4) Assess the impact or severity of each risk.
(5) Determine the overall risk to achieving the objectives of the T&E event.

c. Risks to a T&E event are not limited to items directly comprising the system under test, but also to the encompassing T&E environment and resources, including personnel. All the topics addressed in a TRR are candidates for risk assessment. A risk assessment may also be tailored to focus on specific areas of concern or complexity, such as software, to address the risk of potential failures in a particular domain.

d. The intent of the risk assessment is to assist in determining the jeopardy to an upcoming T&E event, usually not more than 6 months away, due to problems with the system under test or the test preparation process. In particular, the risk assessment will determine if there is a significant likelihood that there are problems in one or more areas. For instance, the risk could—

(1) Prevent completion of the event or make it impossible to answer key T&E issues. This could be the result of the lack of capability, or the inability to complete an event, which is necessary to make the evaluation.

(2) Cause incidents that result in significant harm to personnel or damage to equipment.

(3) Cause the system to be found to be ineffective, unsuitable, or not survivable. However, the risk assessment is not intended to be a pre-assessment of the system's effectiveness and suitability, per se.

e. The T&E events referred to here are often tests. This risk assessment process can also be applied to other appropriate events used in the system evaluation.

Q–51. Risk management

Dealing with risk consists of four basic steps as shown in figure Q–26. The process is iterative and knowledge gained in each application of the process refines the information derived in each step.

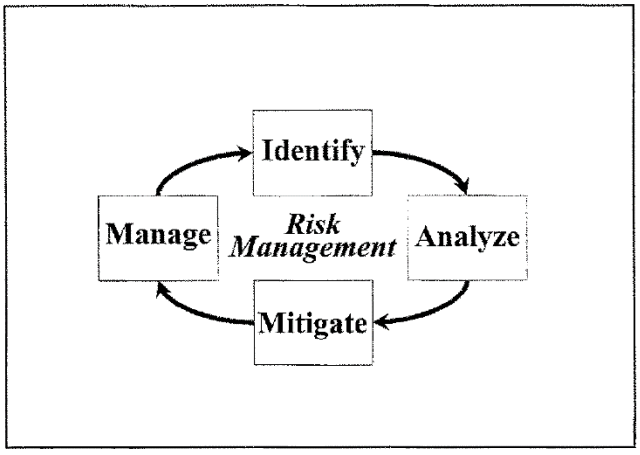


Figure Q–26. Basic risk management process

a. Identify potential risks based on rough estimates of consequence (that is, its adverse affect and its probability of occurrence). At first, risks may be vague and general in nature, and may concern either a process or a product.

b. Analyze each potential risk to more closely define its precipitating event or situation, the likelihood of occurrence of that event, and the consequence in terms of cost, schedule and/or performance. Rank the risks to identify those that must be dealt with in order to succeed. Integrate the risks to identify the major sub-system and system level risks, with special emphasis on integration risks between hardware, software, personnel, and environment elements. The output of this step is an initial risk list.

c. Mitigate the identified risks where possible by identifying mitigation alternatives. Determine the cost and benefits of each alternative in terms of reducing its consequence or reducing its probability of occurrence. Risk mitigation usually involves trading cost, schedule, or performance to reduce the risk. Determine the best set of mitigation alternatives that are affordable and produce the greatest risk reduction for the cost. The output of this step is a list of mitigation alternatives with costs (that is, in terms of cost, schedule, and performance) and benefits (that is, in terms of reduced risk).

d. Manage the remaining risks by selecting and executing risk mitigation strategies (which could include postponing the T&E event), monitoring remaining risks to validate the correctness of the risk assessment, and continuing to assess the program to identify any new risks that appear.

e. Risk assessment for an upcoming T&E event is a special case of the general risk management process. Although the focus is on identifying and analyzing risk, all of the steps of the risk management process will occur. The T&E event risk assessment process, to include one or more TRRs, should be considered as a part of an ongoing risk management operation whose purpose is to give the upcoming T&E event the greatest chance of success. A more detailed view of the risk assessment process is depicted in figure Q–27.

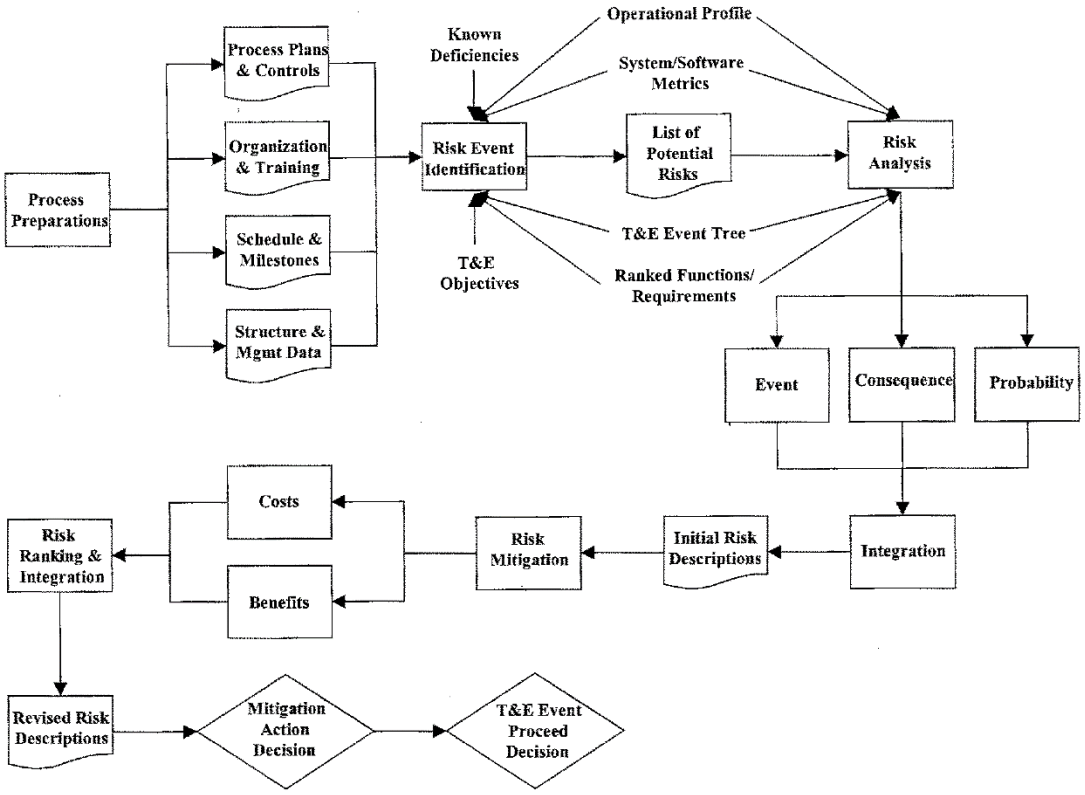


Figure Q–27. Test and evaluation risk process methodology

Q–52. Risk identification

It is impractical to define and analyze every possible risk for any significant activity. The key is to focus on the key risks, which have a significant chance of affecting the T&E event. This is accomplished by first identifying a large group of possible risks which are then narrowed to key risks through further analysis. The risks to a T&E event fall into two major categories: risks in the system under test and risks in the testing environment. In general, define one or more organizing structures that list and organize all elements of the program, and then apply one or more risk identification techniques to each element in order to establish potential risks.

a. Define the risk identification structure. Organizing structures are arrangements of some aspect of the system under evaluation that serve to break the system into assessable elements, ensure complete coverage, and guard against double counting of risk. Possible organizing structures include the following:

(1) *System functional structure.* Examples are a system functional description, requirements list, or UFD. These are used for identifying and ranking mission related consequences.

(2) *Work breakdown structure.* Used for systems that are principally hardware, with software functionality that extends across multiple components. A WBS organization also helps evaluate integration risks, particularly between hardware and software components.

(3) *Software component structure.* Used for systems that are principally software, and whose functionality principally concerns manipulating data and information. An example is a breakdown of CSCIs into computer software units.

(4) *Test event tree and schedule.* Used for identifying safety or implementation related risks to a specific T&E event. The dependencies among events must be known.

b. If more than one assessment structure is used (for example, the software component structure or the system functional structure), it should be possible to map from one to the other. For example, if a particular CSCI is assigned a high risk rating due to uncertainty concerning its development, it should be possible to map back to the associated functionality within the system functional description to determine the potential mission impact. The requirements management process should allow the probability of success for a software element to be associated with the consequences of failure for a set of associated operational functions.

c. If only one structure is used, be sure that both high probability and high consequence concerns within that structure can be identified. While a number of structures may be used for a risk assessment, the final risk organization and presentation should use only one.

d. Risk identification techniques are used to make the initial determination of risks for further analysis. Generally, one or more techniques can be applied to each element of the organizing structure. Integrate the results from these assessments to resolve conflicts, resulting in a list of risks. Rank the list to support culling, if necessary, to produce the list of risks for further analysis.

(1) *Open fault list.* All unresolved problems: system, software, training, and prior TIRs should be included in the potential risk list for further analysis to quantify the potential impact and the probability of occurrence.

(2) *Operational profile review.* Prior test results are a principal source supporting risk assessment for an upcoming T&E event. The test results depict the success of the system in meeting developmental test objectives to date. However, if the upcoming T&E event is an operational test, the usefulness of prior test data depends on the degree to which the developmental test circumstances mirror the operational environments and inputs that will be faced during the operational test. If the operational environment is incorrectly or incompletely represented in DT, the DT test results will not provide an indicator of OT success. In addition, operational situations that are either missing or under-represented in the operational profile may mean that there is uncertainty as to the ability of the system to operate in those situations. These operational situations should be placed on the list of potential risks for further analysis.

(3) *Test and evaluation event tree.* Plans for the T&E event itself, such as the SEP and EDP can be an effective structure for identifying high consequence risks. The T&E event can be displayed as an event tree using the same format as a WBS. Divide the T&E event into separate activities representing the evaluation requirements from the SEP. Further divide the separate activities into the events that must occur to support that activity. Continue to develop to a level low enough to allow assessment of potential failure modes and consequences of failure. Associate relevant testing environment items, such as instrumentation, facilities, support equipment and support personnel, and test player training and availability to the test events including the timing of events per the testing schedule. Risks in the adequacy of the test program to provide for the proper collection of sufficient and valid data for the evaluator to perform a credible, timely analysis and evaluation, and risks to the availability of test resources or pre-test training should be included on the initial risk list for further analysis. Also associate the system or software functions that occur during the activity with each event. Risks that are possible and have a high consequence (for example, risks that involve KPP and COIC), should be included on the initial risk list as well.

(4) *Function or requirements rankings.* One of the quickest and most effective ways to identify risks driven by high consequence is the function or requirement ranking process. Using a requirement list or Critical Mission Functions in the UFD, have operational experts rank the system functions relative to importance if they are not achieved. This ranking is usually based on an assessment of how important that function is to mission accomplishment. With the assistance of system or software development experts, rank the functions relative to the likelihood that they will be fully implemented in the system under development. High-risk functions are then mapped back to the system elements that support them. The associated system elements are placed on the initial risk list unless other risk identification techniques strongly indicate that they will be successful.

(5) *Metrics.* Metrics are the parameters and supporting data that measure progress relative to plan for a development program. The selection and form of the metrics can vary from project to project. It would be unusual, however, for a program to have no metrics, and an indicator of risk.

(a) Each of the metrics listed in section VI of this appendix support an important element of information that is normally necessary for effective program management. If there is no apparent metric dedicated to that management function, determine how the program manager is measuring progress for that aspect of the program. If they are not, associated risk goes up.

(b) The metrics in section VI of this appendix are oriented toward software-intensive systems; however, most of them are readily adaptable to measure relevant hardware or system characteristics. Section VI also contains definitions of software metrics and includes a discussion concerning the types of data within each metric and analysis techniques.

(c) Software metrics generally serve to assess the probability of successful completion of software components. The consequences of risks are determined by identifying the associated functionality of the software components in question, and assessing the impact should those functions fail.

(d) Trends in defect discovery and closure rates (Fault Profiles) and testing coverage of requirements (Breadth of Testing) can provide valuable insight to identify areas of software or system risk.

(e) An individual metric, by itself, does not necessarily indicate the likelihood of future faults. Multiple metrics all pointing toward the same system or software elements, however, clearly indicate a potential risk, which requires additional analysis.

Q–53. Risk analysis

The objective of risk analysis is to define the potential consequences and probabilities of occurrence of a risk with enough specificity that they will support decisions concerning mitigation, including the decision to proceed or not proceed with a test event. Risks may be known or unknown. A known risk is one for which the risk event, the probability and the consequence can be defined with reasonable confidence. Unknown risks are those for which you know that there is a significant consequence but are not sure of the probability or those for which you know that there is a significant uncertainty but are not sure of potential consequences. For example, at the 90 percent confidence level, reliability projections predict one to two new faults will occur during testing but do not predict where they are likely to occur. Unlike known risks, work with ranges for the unknown risks, with the size of the range varying in proportion to the level of uncertainty concerning the risk.

a. Risk analysis techniques are methods to quantify the consequences and probabilities of occurrence of risks. Individual risks are assessed and then integrated into groups of risks associated with larger aspects of the T&E event.

(1) *Failure modes and effects analysis.* In some cases, it may be possible to quantify a risk by identifying the potential failure modes and the effects of failures by these modes. The initial assessment of failure modes is made at the black box or functional level. Evaluate each function for which a risk has been identified to determine the ways in which possible input or processing errors might occur. Once failure modes are identified, the consequences of this type of failure during the T&E event can be quantified, and the likelihood of failure in this limited way can be assessed. For example, a software function may receive target location information and generate range and direction for a cannon to fire on that target during a training exercise. Potential failure modes could include no data, generation of incorrect data but safe data, and generation of incorrect but unsafe data (round lands outside the firing range). Consequence assessment is straightforward. By evaluating the ways in which these failure modes could occur and linking them back to the supporting software elements, it may be possible to assess the probability of occurrence of each.

(2) *Metrics.* Some metrics may be useful for quantifying the probability of occurrence of a particular deficiency, the likelihood of new faults occurring, or the likelihood existing faults will be resolved in a time to meet a scheduled event. For example, an informative indicator of progress is to examine the number of faults, or defects, the software has recently experienced. If there are many unresolved faults or the rate at which problems are being corrected is slowing down, this could pose a risk that not enough problems will be resolved and tested prior to an evaluation event. Figure Q–28 illustrates a fault profile. A risk assessment is taking place in February for a T&E event scheduled in May. The number of defects for System X has grown rapidly in the last few months while corrective action is lagging behind. Even if no new problems were detected, the present rate of resolution would just barely close them all before the T&E event. This would seem to pose medium to high risk. As another example, taking a closer look at the currently open software faults (see fig Q–29), however, reveals that the majority of problems are not serious enough to affect the outcome of the T&E event. Risk due to software faults appears reduced, but not eliminated.

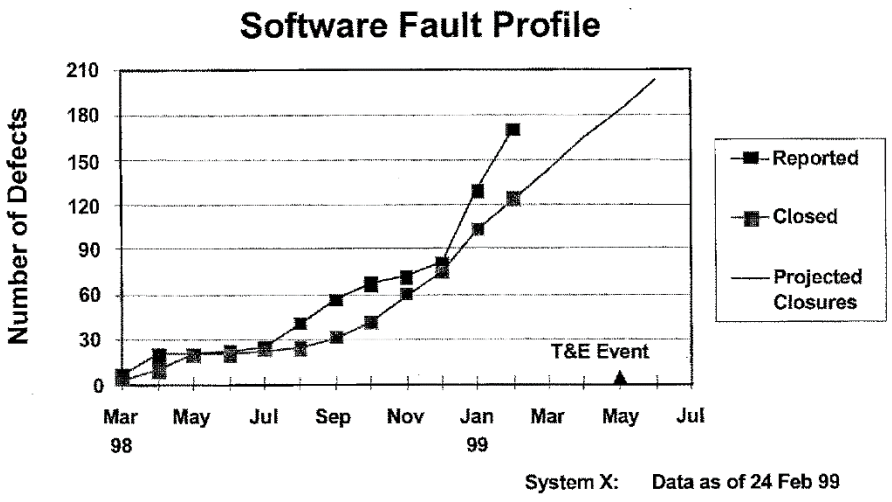


Figure Q–28. Software fault profile metric example

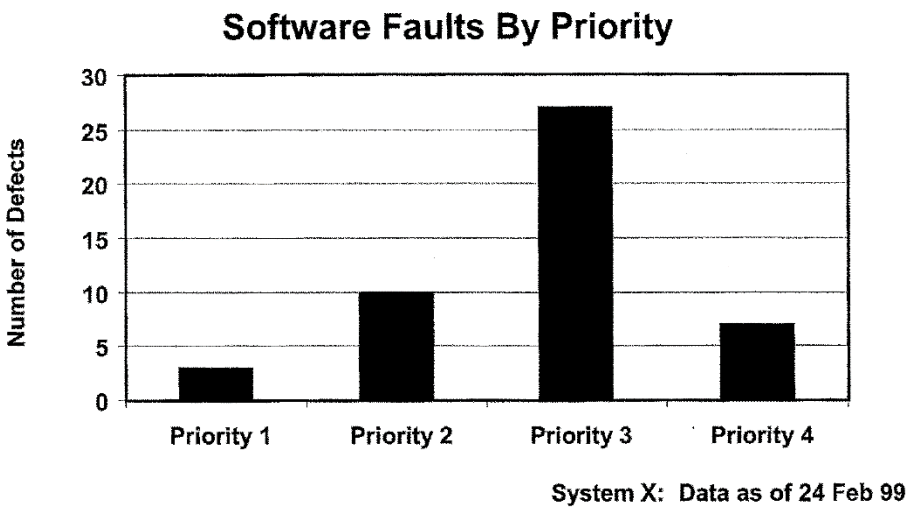


Figure Q–29. Software faults by priority metric example

b. Initial risk identification and analysis activities develop a set of risks for each individual system element at the lowest level considered. These element risks must be integrated at each higher level of the organizing structure in order to understand the total impact, and to identify previously unidentified risks associated with element interfaces. This integration effort requires consideration of the combined risk of several individual risks. Calculating the probabilities of combinations of multiple events can be extremely complex. There are a few simple rules, however, which can provide estimates of combined probabilities and guard against gross logic errors.

(1) The likelihood that an event will not occur is one minus the probability it will occur. For example, if an event has a 25 percent probability of occurrence, there is a 75 percent likelihood that it will not occur.

(2) The probability that a group of independent events will all occur is the product of the probabilities that each will occur. Example. Three separate events each have a likelihood of 50 percent of occurring. The likelihood that all will occur is 12.5 percent (0.5 x 0.5 x 0.5 = 0.125).

(3) The probability that none of a group of events will occur is found by multiplying the probabilities that each will not occur (1 probability that each will occur).

c. Rule 3 helps guard against common risk integration errors.

(1) There is a tendency to assume that, if each element within a system has a low risk, the system must also be low risk. For example, assume there is a system with 50 components, each of which has only a 1 percent chance of experiencing a serious risk. The likelihood that at least one of these risks will occur is approximately 40 percent, which most would consider to be significant. Likelihood that none of these risks will occur = (0.99^{50}) = ~60 percent. Likelihood that at least one will occur is (1 likelihood that none will occur) or (1 - 0.6) = 40 percent.

(2) Risks over an element should not be averaged to determine the risk of the element. Assume, for example, that you are assessing two system elements. One has two risks, each of which has a likelihood of 25 percent of occurring. The other has five risks, also with individual probabilities of 25 percent. While the "average" risk probability for each element is 25 percent, the likelihood of at least one risk occurring in the first element is about 44 percent, while the risk of at least one risk occurring in the second is more than 75 percent. "Average risk" is not a meaningful measure for most risk assessment efforts.

d. It may be useful to rank risks in order to focus on those that are most important. Risk ranking should be done carefully. Risk assessment is often a fairly imprecise process, involving a good degree of subjectivity. Unless the assessment process supports accurate quantification, it is usually better to rank risks in bands (for example, high and medium), rather than to make fine distinctions.

(1) Expected value is often used to determine risk ranking. Expected value is the product of probability of an occurrence times the value of the impact of the occurrence. By itself, however, expected value can hide the actual probability and consequence values and result in poor decisions. Expected value, or any other single value risk representation, should not be used without also showing the associated consequence and probability.

(2) Sample definitions of T&E event consequences and probabilities of occurrence are provided in tables Q–22 and Q–23. Table Q–24 shows a generic expression of expected value for a risk based on these two sets of definitions.

Table Q–22
Severity of risk event occurrence

Severity of a risk event is—	When the risk event causes—
Catastrophic	Mission failure, loss of system or personnel, or completely prevents collection of data necessary to resolve T&E issues.
Major	Severe mission degradation, personnel injury or system damage, or seriously degrades the quality of data necessary to resolve T&E issues.
Minor	Slight mission degradation, personnel injury or system damage, or slightly degrades the quality of data necessary to resolve T&E issues.
Negligible	Less than minor personnel injury or system damage; no mission or T&E data degradation.

Table Q–23
Likelihood of risk event occurrence

Probability of a risk event occurrence is—	When the risk event will—
Very	Occur frequently during the T&E event.
High	Occur several times during the event.
Medium	Likely to occur at some point during the event.
Low	Probably will not occur during the event, but may occur.

Table Q–24
Risk levels

	Severity			
Probability	Negligible	Minor	Major	Catastrophic
Low	Light	Light/mod	Light/mod	Moderate
Medium	Light	Moderate	Mod/heavy	Heavy
High	Moderate	Mod/heavy	Heavy	Heavy/intensive
Very high	Moderate	Heavy	Heavy/intensive	Intensive

Light: Problem that should not affect T&E event objectives.
Moderate: Some impact on the objectives.
Heavy: Substantial impact on the objectives.
Intensive: T&E event objectives cannot be met.

e. In most risk assessments, it is desirable to group risks that apply to the same system element or function in order to estimate the total risk. For example, there may be multiple ways in which specific functional failure could occur, each with its own probability. The risk assessment must determine how likely the functional failure is given all risks in the group.

(1) The simplest technique is to display the risks as a group. This is appropriate when the risks cannot be quantitatively defined. The grouping will at least allow a subjective judgment concerning the likelihood of occurrence.

(2) If the probabilities are well defined or within narrow ranges, it may be possible to compute the probability of occurrence for the combined group mathematically. The new probability, which will be more likely than any of the individual risks, can then be used to represent the overall probability of functional or element risk occurrence. Unfortunately, these computations can be very complex if there are a large number of dependent risks in the group.

(3) When probabilities are defined by broad ranges (for example, probability of occurrence somewhere between 20 percent and 50 percent with the most likely value around 30 percent), it may be possible to assess the combined probability by using a Monte Carlo simulation program. These programs randomly assign values to each risk based on the defined range and distribution within that range, and then calculate the resulting total risk mathematically. They perform this operation a very large number of times to generate the range of possible total risk probability values, along with the likelihood of occurrence for that value (that is, the number of occurrences as a percentage of the total number of trials). Unlike a straight mathematical computation, this technique handles risk dependencies well as long as they can be described.

Q–54. Risk mitigation

Once risks to a T&E event are identified, it may be possible to reduce them prior to the T&E event by judiciously trading cost, schedule, and performance. All T&E event risks should be considered for mitigation alternatives prior to presenting them for a final management decision. Common risk mitigation techniques are—

a. Assumption. Accept the risk without mitigation. This usually means that there is sufficient risk reserve to compensate for the consequence if it occurs. However, assumption may mean that the decision maker is willing to accept failure if the risk is realized. For a T&E event this usually means that the risk does not seriously endanger test objectives, schedule, or safety.

b. Avoidance. Remove the risk by reducing performance requirements, increasing schedule (delaying or extending the test event), or by adding safeguards which make the risk event impossible (for example, physical restrictions on the range of movement of a cannon tube or using M&S for the system evaluation).

c. Transfer. Move the risk to another program element or organization, usually trading cost, schedule, or performance in the process. This includes such actions as accepting previously conducted commercial or other service testing in conjunction with a manufacturer's warranty or moving the support cost risk to the developer.

d. Control. Accept the risk, but put a management process into place, along with contingency plans, which allows effective reaction to the risk if the probability of occurrence increases. This includes such controls as exit criteria prior to and within the test event, and contingency test plans that can be activated if the original plan fails.

e. Research and analysis. Risk is a function of uncertainty. Additional research and analysis can reduce the uncertainty associated with a risk, for example, gaining a better understanding of the frequency of occurrence of trigger conditions, and narrowing the range of potential consequences.

f. Risk reserve. Both the system's PM and responsible T&E organization should maintain an appropriate cost and schedule management reserve in order to deal with assumed risks and the inevitable surprises associated with any significant T&E effort. In fact, the lack of management reserve should be listed as a general risk. The decision as to how much time and money to place in reserve rests primarily with the PM, but it should involve balancing the consequences of not having the reserve if it is needed against the cost of the risk reserve. The T&E organization's management reserve focuses on time and resource contingencies that preserve the ability to adequately conduct and evaluate the T&E event. Most of the risk reserve should be initially allocated against known assumed risks.

Q–55. Risk assessment results and management decisions

a. The results of the T&E event risk assessment described in this appendix, in most cases, are used to support management decisions regarding—

(1) Readiness for the T&E event as a whole.

(2) Areas of concern that may require immediate attention.

(3) Executing risk mitigation strategies for areas that are likely to pose risk during the T&E event.

b. Detailed results of a risk assessment are not usually suitable for presentation at a TRR, but can be valuable supporting material in addressing the various topics in the review agenda.

c. The objective of the final summary of risks is to give the decision maker an understanding of significant risks in terms of their probabilities and consequences sufficient to support a decision to proceed or not with the T&E event. To the degree possible, the DR emphasizes the specific potential impact of the risk on the test event, along with the probability of that impact occurring. For example, if there is a possibility of losing developmental equipment, the cost of replacing that equipment should be shown. If there is a possibility of an early failure, which would force cancellation of the test, the cost and schedule impact of repeating the test should be identified.

d. At a minimum, the risk assessment summary should include the following—

(1) The principal organizing structure used for the analysis: usually the software design or WBS, the functional description, or a test event breakout, along with a summary assessment of risk for each sub-element of the structure.

(2) An assessment over the organizing structure of the percentage of elements that are subject to significant risk (for example, the percentage of MOE/MOP or system functions affected).

(3) A ranked listing of each significant risk, with a description of the probability and consequence for each.

(4) A list of general risks (that is, those for which consequence and/or probability could not be defined, along with an assessment of the possible affect on the T&E event).

(5) A list of possible risk mitigation actions, along with a description of the cost of each action to include schedule and performance impacts, and a description of expected benefits on the targeted risk.

(6) A recommended course of action with regard to risk mitigation, the decision to proceed or not with the T&E event, and assigned responsibilities for carrying out risk mitigation actions such as test plan modification, and monitoring of exit criteria.

e. The risk mitigation step may have resulted in risk control measures, which require management attention. These may include contingency test plans, which have to be prepared, or exit criteria, which must be monitored to ensure that the appropriate action is taken in response. Assign responsibility for these control measures, along with appropriate monitoring to ensure that they are properly implemented.

Section VIII

Test and Evaluation Planning Process for Post Deployment Software Support

Q–56. Post deployment software support purpose

PDSS refers to modifications or upgrades made to a system's software following the system's FRP DR and initial fielding. This section outlines issues pertinent to PDSS and approaches for addressing those issues.

Q–57. Post deployment software support scope

a. This section applies to the phases of production and deployment, operations and support in the system life-cycle model that is defined in DoDI 5000.02.

b. System modifications and upgrades include multi-system changes, block changes, preplanned product improvements, class I ECPs, and system change packages. In this appendix, the modifications of software and computer resources, regardless of how the change is implemented, are referred to as a software change package.

c. System changes that are extensive enough to warrant approval as a major modification in a post FRP DR are not considered PDSS, but a variation of a new program start. The MDA determines which acquisition phase the program should enter.

d. The applicability of procedures in this appendix to any given program and the extent to which they are carried out is dependent on overall system factors, such as deployment philosophy, and the criticality and urgency of a change.

Q–58. Post deployment software support objective

The objective of PDSS is to correct deficiencies. Deficiencies include both problems reported by users or detected during software maintenance, and modifications needed to improve system software to meet new or changed requirements.

Q–59. Post deployment software support issues

a. The PDSS environment generally focuses on correcting reported software problems for systems that are deployed and enhancing the software as system requirements change. The PDSS organization typically collects these changes into a few formal software releases to avoid disrupting the fielded system. Differences in the amount of change to software and timing of software releases should be considered in identifying the scope of total T&E required and the extent of T&E team involvement.

b. Software development activities performed in PDSS are the same as those carried out prior to first fielding. These activities are tailored to reflect the effort required for implementing each software change proposal (SCP), updating pertinent documentation, verifying the SCP, and issuing changes to users. The scope of the change and the criticality of affected software units should be considered in determining the T&E strategy for each SCP.

c. If an SCP does not have operational impact, then the PDSS agent determines the action necessary to support the decision to field the change. The maintenance PM determines—

(1) The scope of software change in the SCP.

(2) The amount of rework necessary to implement the changes.

(3) The amount of testing needed to ensure that new or modified functions operate properly and that no new errors have been introduced.

d. Changes that introduce new or revised operational requirements or changes that may have an operational impact on the system require independent developmental and operational evaluations. Testing must provide the information needed to evaluate the impact of the change.

e. The urgency of delivering a change to user agencies may have an impact on the extent and thoroughness of a given T&E effort.

Q–60. Controlling software changes

a. Changes to the software production baseline are documented in an ECP–S and categorized based on the urgency of the proposed change and the impact on operational mission effectiveness, considerations which are usually classified as either emergency, urgent, or routine.

b. An ECP–S often addresses a set of related problems or change reports. Packages of changes are approved and scheduled for implementation by the appropriate CCB.

Q–61. Scope of testing

a. The developer performs software unit testing and unit integration and testing of the new or modified software units.

b. The developer should repeat some or all aspects of qualification testing to demonstrate that previous requirements are unaffected and new or modified requirements are met.

c. When independent developmental or operational evaluations are necessary, the procedure outlined in paragraph Q–62 below can assist in determining the level of DT/OT needed to support those evaluations. In general, these evaluations are needed when changes in computer resources (hardware, software, firmware, or communications)—

(1) Have a physical impact on either the operation or support of the system.

(2) Have a noticeable impact on the system's operational effectiveness, suitability, and survivability, affect user interfaces, or impact critical mission functions.

(3) Cumulatively affect 15 percent or more of the software units in the system since the last time such evaluations were made.

Q–62. Determining test support needed for independent system evaluation

a. The procedure described in this paragraph assesses various aspects of the deployed system's T&E history, current maintenance environment, and potential impact of the SCP on the system's operational effectiveness and suitability. The intimate knowledge and informed judgment of the test IPT and CCB principals should guide the decisions made in applying the procedure described in this paragraph and in interpreting its results.

b. There are several steps in the procedure—

(1) Determine the potential problems for an SCP using table Q–25.

(2) Determine the likelihood of each problem, using table Q–26.

(3) Determine the severity of each problem, using table Q–27.

(4) Combine the findings of tables Q–26 and Q–27 to determine the location in the matrix of table Q–28. Table Q–28 will define the amount of testing needed to adequately test the new software that addresses the problem.

(5) Tailor the DT and OT MOPs and MOEs to address the problem.

Table Q–25
Example checklist of potential problems in implementing a software change package

Items concerning—	Potential problem in implementing a software change package
1. System performance	a. Does the software change affect the way the system operates? b. Does the software change affect the system's operational capability, to include— (1) MNS, ORD, or operational MP? (2) Qualitative and quantitative personnel requirements? (3) The operational environment? (4) Critical operational issues? (5) Operating procedures? c. Does the software change affect a critical mission function of the system? d. Does the change affect safety or security features? e. Does the change affect the system's COIC or AIs and criteria? f. Does the change affect the system's CTP?

Table Q–25
Example checklist of potential problems in implementing a software change package—Continued

	g. Will there be a significant change in the system's throughput? In the throughput of particular components? h. Will significant changes be made to support software (operating system or database management system)?
2. Interoperability	a. Does the change affect interfaces with any other systems? b. Is code changed to interface with non-developmental or off-the-shelf software? c. Is there adverse change in system performance caused by execution or management of peripheral devices? d. Are protocols for communication links affected? e. Are there changes in the input or output formats? f. Does the software modification impact other hardware/software interfaces? g. Will procedures for exchanging information with other systems be changed? (1) Within the battlefield functional area? (2) With other battlefield functional areas? (3) With strategic or theater level systems? (4) With joint systems? (5) In accordance with international agreements?
3. Usability	a. Does the change affect interfaces with any other systems? b. Is code changed to interface with non-developmental or off-the-shelf software? c. Is there adverse change in system performance caused by execution or management of peripheral devices? d. Are protocols for communication links affected? e. Are there changes in the input or output formats? f. Does the software modification impact other hardware/software interfaces? g. Will procedures for exchanging information with other systems be changed? (1) Within the battlefield functional area? (2) With other battlefield functional areas? (3) With strategic or theater level systems? (4) With joint systems? (5) In accordance with international agreements?
4. System support	a. Does the change affect the system's support facilities (for example, software tools, support personnel, support equipment, and support documentation)? b. Does the change affect built-in test equipment? c. Will there be a change in the organization responsible for PDSS? d. Does the developer lack experience with the tools or products to make the change?
5.Software metrics	a. Do any requirements remain untested? b. Were there any catastrophic or major problems (as defined in table Q–27) experienced during last deployment of the system? c. Did any catastrophic or major problems occur during any previous testing of this change package? Do any priority 1 or 2 problem reports remain open? d. Is the number of SLOC added, deleted, or modified greater than 10% of the total fielded SLOC? e. Is the use of computer resources likely to exceed the capacity target upper bound? f. Have all changed requirements been traced to code and test cases? g. Does the system currently meet its MTBF requirements?

Table Q–25
Example checklist of potential problems in implementing a software change package—Continued

	h. Is the change package more than 15 percent behind schedule?

Table Q–26
Determining the likelihood of a problem

Probability of problem is—	When the problem will—
Very High	Occur frequently in the system's life
High	Occur several times in the system's life
Medium	Likely occur at some time in the system's life
Low	Probably not occur in the system's life, but may occur

Table Q–27
Determining the impact of a problem

Impact of problem is—	If the problem causes—
Catastrophic	Mission failure, loss of system, or loss of personnel
Major	Severe mission degradation, personnel injury, or system damage
Minor	Slight mission degradation, personnel injury, or system damage
Negligible	Less than minor personnel injury or system damage; no mission degradation

Table Q–28
Checklists for integrated product team and configuration control board to address probability and impact of a problem

	Impact of problem or risk			
Probability of problem or risk	Negligible	Minor	Major	Catastrophic
Low	Light	Light/moderate	Light/moderate	Moderate
Medium	Light	Moderate	Moderate/heavy	Heavy
High	Moderate	Moderate/heavy	Heavy	Heavy/intensive
Very high	Moderate	Heavy	Heavy/intensive	Intensive

Test requirements, based on level of risk—
Intensive: Up to and including full repeated DT/OT from Milestone C plus changes
Heavy: DT with significant OT
Moderate: DT with OT excursions
Light: DT

c. Examine all DT and OT MOPs needed to adequately test the SCP to plan the necessary test events. It is the responsibility of the evaluator to determine the most effective mix of DT and OT to support their evaluations. This could entail substantial use of developer test information, concurrent DT/OT exercises, simulations, or other strategies.

d. It is recommended that the checklist (that is, table Q–25) be used several times during the course of SCP planning and implementation to improve the estimate as more information becomes known. The last check should contain no "unknown" answers—mark these as "yes" to represent worst case.

Q–63. Other considerations

a. System post-deployment review.

(1) The PM should plan to convene one or more system post-deployment reviews during PDSS to determine how well the system is functioning. The first system post-deployment review is recommended approximately 6 months after all initial units are equipped or all site installation is completed. The review should assess—

(a) How well the operational system is satisfying user requirements to meet the stated mission.

(b) The degree to which the system operates as the user expects and provides the services expected.

(2) The PDSS agent uses system post-deployment review results to identify problem areas and develop changes that will improve system performance and usability. Additional reviews throughout the deployment and operations phase provide assurance that the SCPs continue to satisfy user needs and improve overall system quality. The initial system corrective actions, problem areas, and changes dictate the content of the reviews.

b. Emergency changes. In response to critical situations, emergency changes may need to be released to the field within 48 hours. While all changes must undergo validation, verification, and regression testing, emergency changes to deployed systems may not require formal DT or OT prior to release. All emergency changes, however, will undergo formal testing with the next planned updates. The PM, with the concurrence of the system user, may only be capable of performing limited testing of emergency software corrections prior to granting release.

c. Test reusability. Test cases, data, and procedures stored in developer software development files may be necessary or desirable for enabling the LCSEC/PDSS agent to retest software during maintenance more effectively. If so, the appropriate items should be included in the technical data package delivered by the developer.

Section IX

Software Problem Change Report Process

Q–64. Software problem change report

a. A software PCR is the formal description of any problem that has been observed in an "approved" software product that has completed some level of evaluation and has been placed under configuration control. Depending on the phase of the software development effort, the approved product baseline may be a set of requirements documents or a complete software program.

b. Software PCRs are used not only to identify problems, but also to track the status of problems until they are resolved. It is important for evaluators to understand the software PCR process because PCRs are the most common measure of software product quality.

c. Other common terms for software PCRs are STR, software problem report, and software problem and defect.

Q–65. Information provided in a software problem change report

a. Figure Q–30 provides a detailed description of the information that is typically provided in a software PCR. The system evaluator reviews individual software PCRs to ensure proper priority classification criticality. The team must be aware of the overall status of software PCRs on a project to assess the magnitude of the problems and their potential impact. The types and numbers of problems can measure the magnitude of software problems. The potential impact of software problems can be defined by the criticality of the problems and the probability that they will be resolved before the system is fielded. Figure Q–31 describes a common classification scheme to identify the type and criticality of software problems.

A software PCR typically includes this information-

a. **Problem description**: A detailed description of the problem and its symptoms as well as a summary or short title for reporting. The major functions affected or impacted by the problem should be identified.

b. **Configuration control identification**: Identification of the software, such as build, version and software configuration item and possibly identification of elements of the test environment.

c. **Operating environment**: The type of environment in which the problem was detected, such as the type of test that was occurring and whether the software was running on a test platform or operational hardware.

d. **Time of occurrence**: The date, and possibly time of day, the problem was detected.

e. **Problem category**: The type of software problem, usually a standard category as described in figure Q-31.

f. **Problem priority**: The severity of the problem, often expressed in terms of user or mission impact that is defined by a standardized category as described in figure Q-31.

g. **Problem status information**: As a PCR is processed through the corrective action system; it passes through a number of steps or stages before it is officially closed.

(1) **Resolution status.** The most important stage to the independent evaluator is the resolution status, where a configuration accounting is made. Examples of resolution status are: problem logged, problem analysis complete, code modified and unit tested, modification integrated and tested, regression testing complete, software change package complete, problem closed.

(2) **Time of closure**. The date the problem completed all its steps through the corrective action process and was officially closed by the configuration control authority.

(3) **Reason for closure**. Not every software PCR requires modifications to code so as to resolve. It can be useful to have information about reasons for closure in order to refine PCR analysis. Examples of closure reasons include: software product(s) modified; documentation updated (for example, user manual); duplicate problem; and administrative closure (such as the problem cannot be re-created.)

Figure Q–30. Typical information provided in a software problem change report

Evaluating the status of software PCRs requires knowledge of the types of problems identified and their criticality to the project. This evaluation is facilitated by use of a standardized classification for the type (category) and criticality (priority) of each PCR. The most common classification schemes for problem category and priority definitions are:

a. Classification by Category.

(1) Requirements problem. The software does not operate according to requirements documentation and the documentation is correct.

(2) Design problem. An error or deficiency has been identified in the software design.

(3) Code or software problem. The software does not operate according to correct requirements documentation.

(4) Documentation problem. The problem is identified in the supporting documentation; including management plans, test plans, test descriptions, user, operator, or maintenance manuals.

(5) Other problem. Any other type of problem that may be identified.

b. Classification by Priority.

(1) Priority 1. A software problem that prevents the accomplishment of an operational or mission-essential capability or jeopardizes personnel safety.

(2) Priority 2. A software problem that adversely affects the accomplishment and degrades performance of an operational or mission essential capability and no alternative work-around solution is known.

(3) Priority 3. A software problem that adversely affects the accomplishment and degrades performance of an operational or mission essential capability, but an alternative work-around solution is known.

(4) Priority 4. A software problem that is an operator inconvenience or annoyance and does not affect a required operational or mission essential capability.

(5) Priority 5. All other errors.

Software projects may use various other priority classification schemes. For example, projects developing software for information technology systems may use only three levels of priority, with the terms Emergency, Urgent, and Routine used to identify the criticality of software PCRs.

Figure Q–31. Problem change report category and criticality codes

b. A PCR can only be written if a problem has been observed. The evaluator must always assess the status of software PCRs with an understanding of the capability of the project to find and identify problems. The capability to identify problems includes not only the effectiveness of the software test program, but also the ability of the technical and management processes to identify and resolve problems in all related elements of the project, including systems requirements and documentation. The number and age of unresolved software PCRs reflect the ability of the developer to resolve problems. This information gives the evaluator an indication of the likelihood that software problems will be resolved before the system is fielded.

Q–66. The process for managing software problem change reports

a. Every software developer and maintenance activity must implement a corrective action process to manage the problems that are detected in the approved software product baseline. The corrective action process must be a "closed-loop" process in which software PCR forms are written on all detected problems, monitored in a tracking and reporting system, and marked as closed when the problem is corrected. The same procedures apply for both hardware and software PCRs.

b. A software PCR usually can be written and submitted by anyone, including system developers, system operators, testing personnel, and maintenance or installation, integration, and production personnel. A system evaluator should ensure that, at a minimum, the acquisition or maintenance agent manages an effective software PCR, using the following specific steps:

(1) Designate a configuration management (CM) authority to determine if the PCR is very minor or trivial, or if action should be taken. Based on knowledge of technical and program management issues on the project, the CM

authority approves or rejects very minor or trivial PCRs. In general, any change that does not affect performance, requirements, or system interfaces may be considered minor.

(2) If the CM authority determines that action should be taken on a software PCR, the next step is to enter the PCR into a tracking system, which is usually a database file that is managed by the CM authority. Only the CM authority can subsequently modify or delete a PCR that has been submitted.

(3) The next step of the CM authority is to decide if the required change should be brought before the CCB. The CCB must approve any problem or proposed change that will require additional project resources or will impact other system or software elements within or outside of the project. These changes are usually called Class I changes to distinguish from Class II changes that can be approved by the CM authority without review by the CCB. The criteria used to identify Class I and II changes are established by the CCB for each project.

(4) The CM authority periodically produces a report from the PCR file on the status of all PCRs that have been submitted and are being processed.

(5) A copy of every Class I software PCR will be provided to the CCB, containing a technical description of the proposed change and the associated cost.

(6) After reviewing the completed Class I software PCR form, often called a proposed software ECP, the chairperson of the CCB will make the final decision to convene a CCB meeting for the PCR. The CCB meetings are usually scheduled on a regular basis to review a group of PCRs or proposed ECPs at one time. A CCB meeting will be convened immediately for the most critical PCRs.

(7) If the CCB approves a software PCR or proposed software ECP, the result is an approved and funded software ECP that typically must be implemented as soon as possible.

(8) The final step for a software PCR in a corrective action process is to document that the corrective action for both Class I and II changes have been implemented and tested.

Q–67. Evaluator responsibilities for software problem change reports

An evaluator must assess the status of software PCRs throughout the software life cycle, especially prior to each upcoming test event. As a minimum, the evaluation should consider the effect of unresolved problems that remain in the software baseline that will be tested, the trends in the software PCRs that have been reported, the potential impact on the future of the project, and the status of corrective actions. The following paragraphs provide tips for the evaluator in assessing the software PCR status.

a. The effect of unresolved problem change reports.

(1) Unresolved priority 1 or 2 software PCRs may cause safety hazards or prohibit the system from performing critical mission functions. These PCRs should be eliminated before any system-level test is performed.

(2) Although testing is usually performed with unresolved priority 3 PCRs, the evaluator should review the impact analyses that are submitted with each priority 3 PCR. A priority 3 PCR has the same potential affect on the system critical mission functions as a priority 2 PCR, but a workaround exists to avoid the system consequence. The system evaluator should evaluate the cumulative effect of the workarounds and the potential volume of non-standard actions that will be required to achieve the prescribed mission performance.

(3) Too many unresolved low-priority PCRs may have a cumulative impact that will degrade the system performance.

(4) If a software item affects a critical mission function, a software reliability analysis may be justified for additional insight into the probability of a failure occurring during an upcoming test event or in the final product.

b. Trends in software problem change reports.

(1) A trend that shows an increasing number of PCRs that are not quickly resolved indicates that the developer's process cannot deliver a high-quality product. PCRs should be resolved as quickly as possible to allow adequate regression testing and ensure problems do not occur when the changes are integrated into the approved product baseline.

(2) The system evaluator should be aware of software products or items that have experienced many problems. Experience has shown that these items are usually difficult to develop and are more likely to contain errors that are not detected.

c. The status of corrective actions.

(1) Evaluating the status of corrective actions must consider the effectiveness of retesting the software changes that have been made to resolve PCRs. This retesting process is also known as regression testing. Regression testing is needed to ensure that changes have been correctly implemented and that additional problems have not been introduced by the changes. Regression testing consists of repeating a subset of the previous test cases and test procedures after software changes have been made.

(2) The minimum requirements for regression testing are—

(a) All test cases and test procedures in which the software problem was experienced in the previous testing have been repeated, and the results have met acceptance criteria and have been recorded.

(b) All test cases and test procedures for software that is affected by the changes to resolve the software PCR have been repeated, even if there were no problems during the previous testing of that software.

Appendix R

Department of Army Test Facilities

R–1. Overview of Army test facilities

a. This appendix provides synopses of DA test facilities for quick reference. More detailed information on the capabilities may be obtained from the test facility or its parent command.

b. The Army maintains and operates six of the DoD MRTFB facilities, which are regarded as "national assets," that are maintained under uniform guidelines primarily for DoD T&E support missions and functions. The SMDC operates two MRTFBs (the HELSTF and the RTS). ATEC operates the remaining four MRTFB activities (ATC, DPG, YPG, and the WSMR, which includes the EPG) as well as two other test facilities (U.S. Army Aviation Technical Test Center (ATTC) and the RTTC). A synopsis of each follows.

R–2. U.S. Army Aberdeen Test Center

ATC, located on Aberdeen Proving Ground, Maryland. It is a multipurpose test center with diverse capabilities and the Defense Department's lead agency for developmental land combat and direct-fire testing.

a. ATC provides a single location where combat systems can be subjected to a full range of tests from automotive endurance and full weapons performance through induced environmental extremes to full-scale live fire vulnerability/survivability/lethality testing using an extensive array of test ranges and facilities, simulators, and models. Testing is conducted on both full systems and system components and includes armored vehicles, guns, ammunition, trucks, bridges, generators, night vision devices, individual equipment such as boots, uniforms, and helmets, and surface and underwater naval systems.

b. ATC offers numerous exterior and interior firing ranges, automotive courses, chambers simulating various environmental conditions, two underwater explosion ponds, sophisticated non-destructive test facilities, multifunctional laboratories, and an extensive industrial complex that includes maintenance and experimental fabrication capabilities. Ammunition is prepared in on-site ammunition plants to meet customer needs. Experienced personnel also conduct and/or support tests at other locations throughout the world with extensive mobile instrumentation.

c. ATC serves as the host for the Army Pulse Radiation Facility (APRF), the nation's only combined ionizing nuclear radiation environmental simulation laboratory capable of supporting DT and OT from discrete electronic components up through complete systems at full threat specification levels.

R–3. U.S. Army Aviation Technical Test Center

ATTC, located at Cairns Army Airfield, is a tenant of the U.S. Army Aviation Center at Fort Rucker, AL. With nearly 50 years of experience in the field of aviation DT, it is a highly flexible test organization that provides a high degree of test mobility on the total integrated aviation system.

a. ATTC conducts developmental flight-testing and airworthiness qualification testing on subsonic fixed- and rotary-wing aircraft, aircraft systems and subsystems, and aviation support equipment. Flight-testing focuses on assessing system performance, system integration with the aircraft and other installed systems, system safety, Soldier/machine interface, HFE, and logistics supportability. Airworthiness qualification testing, which is performed by experimental test pilots, assesses the flight characteristics and handling qualities of the aerial vehicle and its in-flight performance. Because of the test mobility inherent to aviation, ATTC has the capability to conduct extensive testing at off-site locations throughout the continental U.S., where specific test capabilities or climatic conditions are required.

b. ATTC facilities include three hangars and 12 support shops located on Cairns Army Airfield and access to two hard-surface runways. The ATTC maintains a fleet of 16 test bed aircraft, representing the Army's fielded aviation systems. The one-of-a kind Helicopter Icing Spray System allows ATTC to evaluate airframe icing characteristics and de-icing/anti-icing system performance in artificial icing conditions.

R–4. Central Test Support Facility

The CTSF, located on Fort Hood, Texas, is operated and funded by the Program Executive Office for Command, Control and Communications-Tactical. It is identified as the intra-Army interoperability testing facility to perform the communications/data interfaces testing. The mission is to test all Army C4I systems to ensure interoperability in accordance with Intra-Army Interoperability Certification Policy, Acquisition Executive Memorandum "Intra-Army Interoperability Certification," Secretary of the Army, Information Systems (IAA) (SAIS–IAA), dated 3 December 2000. The CTSF testing process is modeled after the ATEC OTC guidelines.

a. CTSF testing in support of the intra-Army certification process will not duplicate or limit testing conducted by the JITC, ATEC, or other test activities. The CTSF testing bays are instrumented with EPG collection and reduction

devices. Partnership enables the testers to integrate the instrumentation with the Army Battle Command System systems.

b. The CTSF conducts the required intra-Army interoperability certification testing and provides the test results to the Army's certification authority, CIO/G–6.

R–5. U.S. Army Dugway Proving Ground

DPG is located approximately 75 miles southwest of Salt Lake City, UT, in the Great Salt Lake Desert. This remote, isolated installation serves as the Defense Department's primary chemical and biological defense testing center.

a. DPG conducts exploratory and developmental tests of chemical and biological defense systems, smoke and obscurant munitions and delivery systems. Testing is also conducted on all materiel commodities to assess chemical/biological hardness and contamination/decontamination survivability.

b. DPG's facilities include indoor laboratories and test chambers, as well as outdoor test sites and extensively instrumented test grids for use with simulants. State-of-the-art chemical testing facilities support indoor testing of largescale military vehicles and aircraft in hazardous environments as well as simulant-only testing. The Life Sciences Test Facility has the only chamber in the United States designed to test against potentially lethal agents in aerosol form. Other facilities allow testers to evaluate the environmental results from open burning and open detonation, accurately replicating real-world disposal operations. The DPG range also includes extensive mortar and artillery firing ranges for testing smoke and illumination rounds.

R–6. High Energy Laser Systems Test Facility

The HELSTF is the DoD high-energy laser (HEL) test activity within the MRTFB. It is the only approved above-the-horizon dynamic HEL test range. The Laser Clearinghouse has accredited HELSTF for decentralized predictive avoidance for dynamic HEL testing. HELSTF has a complete set of HEL diagnostic instrumentation, including an outdoor explosive test range, an indoor coupon test area, and a large vacuum chamber (50-foot diameter, 650,000-foot altitude capability). HELSTF has a complete carpentry and metal shop for fabrication of test support equipment and a complete Atmospheric Sciences department to collect atmospheric data during all tests and to provide pre-test prediction of atmospheric propagation based on M&S and databases maintained at HELSTF. The Mid-Infrared Advanced Chemical Laser (MIRACL), a megawatt class CW Deuterium Fluoride laser, is able to test in all these test areas through a complete set of beam steering optics. In addition, the SeaLite Beam Director is capable of placing the MIRACL beam on a variety of static to highly maneuverable tactical targets for research and development and proof-of-principle testing. The SeaLite Beam Director also serves as the most accurate and longest range imager for ballistic missile tests conducted at WSMR, NM.

R–7. U.S. Army Kwajalein Atoll/U.S. Army Ronald Reagan Ballistic Missile Defense Test Site

USAKA/RTS is located in the Republic of the Marwill Islands and encompasses approximately 750,000 square miles (although the total land area is only about 70 square miles). Its isolated location and specialized state-of-the-art data-gathering devices make USAKA/RTS uniquely qualified for ballistic missile testing and space-object tracking, with minimal safety and environmental constraints. USAKA/RTS provides range radar tracking, impact scoring, recovery, and telemetry data collection for intercontinental and theater ballistic missiles, orbital objects, and reentry vehicles. Facilities include a broad range of ground and mobile instrumentation, radar tracking and imaging, telemetry, and splash detection radar, and large aperture optical sensors. Intercontinental ballistic missiles can be launched from California (4,840 miles), intermediate-range missiles from Hawaii (2,430 miles), shorter range theater missile defense-type missiles from Wake Island (730 miles), and other alternate launch sites (240–450 miles). The natural configuration of the atoll (more than 90 islands forming the world's largest lagoon) facilitates tracking and recovery of reentry vehicles and local launches with minimal safety and environmental constraints.

R–8. Redstone Technical Test Center

The RTTC is located on Redstone Arsenal in northern Alabama, adjacent to the high technology community of Huntsville. It is the Army's tester of small rockets and missiles.

a. RTTC conducts performance, quality assurance and reliability testing of small rockets, missiles, rocket and missile components, and associated hardware. It is unique in its ability to test electrical, electro-optical, mechanical and explosive components for product assurance, and verify component, subsystem, and system performance before committing to flight testing. All types of natural and operationally induced dynamic, environmental, and electromagnetic testing can also be performed. RTTC is also the primary lightning effects tester for munitions and ordnance in DoD.

b. Located in the foothills of the Appalachian Mountains, RTTC's highly instrumented open-air ranges provide an uncluttered environment. Facilities include fully instrumented flight ranges, dynamic warhead test sled tracks, static

rocket motor test stands and a full range of dynamic, climatic, electromagnetic and lightning facilities for testing missiles and weapon systems. Highly automated laboratory facilities are available for testing all types of weapons components and subsystems under realistic climatic and dynamic conditions. RTTC operates the Army's largest rocket motor static test facility.

R–9. Virtual proving ground

The VPG is throughout the DTC. The VPG is a composite of facilities and technologies that enhance DTC's test program with the aid of computer modeling and realistic simulations. The methods and technologies used by the VPG to test emerging military equipment and systems are undergoing a far-reaching transformation, one that parallels the transformation that is taking place within the Army and the other military services.

R–10. U.S. Army White Sands Missile Range

WSMR operates two separate testing ranges. WSMR, the main testing range that includes the headquarters, is located in the Tularosa Basin in south central New Mexico, near the communities of El Paso, Las Cruces, and Fort Bliss, TX. The EPG is located on Fort Huachuca, in southeastern Arizona near the foothills of the Huachuca Mountains. EPG also has field offices at Fort Lewis, WA and Fort Hood, TX.

a. U.S. Army White Sands Missile Range.

(1) WSMR is primarily a missile range for testing ballistic and guided missiles, and air defense systems, but it also supports a variety of testing needs. These include the full range of electromagnetic effects and nuclear environments testing; artillery and associated command and control systems; aircraft (fixed-wing) armament; and temperature, shock, and vibration effects. As the nation's largest overland range, WSMR provides the opportunity for post-test analysis on recovered debris.

(2) WSMR has more than 1,500 precisely surveyed instrumentation sites with high-speed cameras, tracking telescopes, interferometer systems, and radar and telemetry tracking/receiving stations to collect data during testing. Laboratory facilities include environment, weapon systems simulation, guidance and control, propulsion, climatic, metallography and microbiological. The Lightning Test Facility provides direct and near strike capability for systems under test. In addition to on-post missile and rocket launch sites, the range has developed facilities in New Mexico, Utah and Idaho for long-range firings that impact on WSMR.

b. U.S. Army Electronic Proving Ground.

(1) EPG is the Army's principal center for DT of command, control, communications, computer and intelligence (C4I) equipment and systems. It also conducts tests on EW, optical/electro-optical, unmanned/micro-aerial vehicles, global positioning systems, and aircraft navigation and avionics systems. Test capabilities include the full spectrum of electronics testing—from tests of subsystems such as antennas, transceivers or switches to the entire system. EPG has the capability to perform EMC and electromagnetic vulnerability (EMV) analyses of tactical electronic equipment and systems to include generation of realistic friendly and enemy electromagnetic battlefield environments. Instrumented range services include video and telemetry tracking, position location via radar and position location systems, air surveillance and tracking, and meteorological monitoring.

(2) EPG maintains a full-service, highly instrumented test range and can track and collect data from all types of air and ground systems. Facilities include an electromagnetic environmental test facility, environmental chambers, a stress loading facility to measure the full load performance of communication systems, an EMI/EMC/Transient Electromagnetic Pulse Emanation Standard (TEMPEST) test facility, and many unique, specialized facilities for testing of antennas, radar, unmanned aerial vehicles, and computer software. The surrounding mountain ranges create a natural and effective barrier to outside EMI and allow the unrestricted use of a wide range of frequencies.

R–11. U.S. Army Yuma Proving Ground

YPG is located in southwestern Arizona in the Sonoran Desert, approximately 24 miles northeast of the city of Yuma. YPG is assigned the Cold Regions Test Center (CRTC) and mission and the Tropic Regions Test Center (TRTC) mission, in addition to its desert environment test mission.

a. U.S. Army Yuma Proving Ground.

(1) YPG is the lead test center for extreme natural environment testing. YPG also has the capability to perform as a general purpose proving ground and functions as a DoD MRTFB. YPG is located within a road, rail, and air network, offering rapid access to its testing and training areas. Additional access is offered through MCAS Yuma, approximately 25 miles south. YPG has priority of use on the seven Restricted Airspace Areas overlying its range area and the KOFA Game Range. It includes five major types of landscape, characterized as rugged mountains, moderately rugged mountains, rugged hills, alluvial fans, and alluvial aprons and plains. YPG is divided into two major range areas, with desert environment and desert automotive testing balanced between the two, as follows:

(a) The KOFA Firing Range Complex offers customers up to 75 km firing range coupled with 24-hours-per-day/7 days-per-week airspace control. KOFA Range is an integrated test complex for open air testing for direct fire weapons, artillery, mortars, mines and countermines, demolitions, and small missiles. KOFA Range has 21 fixed, permanent firing positions, over 310 surveyed firing points, and 13 improved and dedicated explosive and non-explosive impact fields, making siting tests, observing projectile impact, and recovery of components very efficient. Ammunition is prepared in on-site ammunition plants to meet customer needs. Conditioning boxes and chambers provide rapid turn-around for increased firing rates.

(b) Cibola Range is a highly instrumented rotary-wing aircraft armament range in the United States. There are 11 drop zones for personnel, hazardous material (to include live ammunition) and multi-purpose airdrop testing supported by Laguna Army Airfield, Castle Dome Heliport, and MCAS Yuma. Laguna is capable of handling all current U.S. military transport and cargo aircraft. A highly instrumented helicopter armament test range, direct fire and moving target ranges, environmental chambers, a modern mine and demolitions test facility, and over 200 miles of improved road courses for testing tracked and wheeled military vehicles are also located on the North-South range. The Cibola Range's 18 by 40 mile range system provides near-sea-level density altitude conditions typical of many of the world's deserts.

(2) The YPG desert environment testing and desert automotive test facilities provide the ideal location for testing individual and Soldier support equipment and automotive systems and components under harsh, desert conditions. There are eight special desert terrain test courses, prepared test slopes and obstacles, and a 2–1/2-mile paved dynamometer course available for automotive testing. These are backed by vehicle fording basins, swim testing facilities, fuel and lubricant testing, and instrumentation capabilities available for wheeled and tracked vehicles. The Mid-East test course is a grueling 22-mile desert terrain course that simulates conditions found in the world's deserts.

b. Cold Regions Test Center. CRTC is located at Fort Wainwright, AK. CRTC offers a full range of test capabilities and professional expertise for temperate, Basic Cold (-5 °F to -25 °F) and Cold (-25 °F to -50 °F) natural environment testing for Army systems. These include combat and tactical vehicles, infantry and special operations weapons, ammunition, missiles, CIE, power generation and decontamination equipment, and direct and indirect fire weapons. It operates over 670,000 acres of range, and almost all forms of individual subarctic environments (to include rugged mountains, tundra, glacial stream beds, deep forest, and snow and ice fields) are available within 50 miles of Fort Greely. CRTC is the only U.S. test site that realistically combines the elements of a winter battlefield with a test season long and cold enough to guarantee suitable test conditions. The winter test window runs from October to March, with the coldest temperatures usually experienced in December and January. Temperate testing, approximating the Northern European climate, is available from April through September. CRTC retains priority of use on airspace overlying its test ranges.

c. Tropic Region Test Center. TRTC is headquartered at YPG, with its primary tropic test facilities located in Hawaii at Schofield Barracks. With the 1999 closure of Army tropic testing facilities in the Republic of Panama, tropic test facilities are currently being reestablished over a wide geographic area. Testing will be performed on-site, with people and equipment safaried from YPG or other sites as needed. TRTC conducts humid tropic tests on a wide variety of military systems, materials, weapons, and equipment of all conceivable types, sizes, configurations, and uses, to determine the effects of tropic conditions on materiel, Soldier performance, and reliability. The combined factors of heat, humidity, solar radiation, insects, fungus, bacteria, and rainfall can quickly reduce the performance of both Soldier and machine and corrode materials beyond utility. The Army Research Office study performed to validate tropic test sites indicates that Hawaii meets many of the tropic conditions required; however, certain tests, notably those dealing with sensors and communications systems, require extreme conditions such as those found in the Republic of Panama. For this reason, YPG has worked through the State Department and negotiated Cooperative Research and Development Agreements with Panamanian universities for testing and research on sensors, communications equipment, and medical operations.

Appendix S

Live Fire Testing

S–1. Overview of live fire testing

This appendix provides general guidelines for the planning, conduct, and documentation of the testing portion of Army FUSL LFT&E programs. The responsible testing agency (generally ATEC's DTC for ground systems, ARL/SLAD for aviation systems and SMDC for integrated missile defense, intercontinental ballistic missiles, space launch, and HEL systems) has the overall responsibility of ensuring that assigned programs are conducted in a timely and cost efficient manner while maintaining the integrity of the test process. See appendix J for LFT&E strategy development discussion.

S–2. Live fire test definitions

a. The term full-up system level testing is that testing that fully satisfies the statutory requirement for "realistic survivability testing" or "realistic lethality testing" as defined in 10 USC 4172. The Defense Acquisition Guidebook further defines FUSL testing as follows:

(1) Vulnerability testing conducted, using munitions likely to be encountered in combat, on a complete system loaded or equipped with all the dangerous materials that normally would be on board in combat (including flammables and explosives), and with all critical subsystems operating that could make a difference in determining the test outcome; or

(2) Lethality testing of a production representative munition or missile, for which the target is representative of the class of systems that includes the threat, and the target and test conditions are sufficiently realistic to demonstrate the lethal effects the weapon is designed to produce.

b. Survivability is the capability of a system and crew to avoid or withstand a manmade hostile environment without suffering an abortive impairment of its ability to accomplish the designated mission. Survivability consists of susceptibility, vulnerability, and recoverability. The focus of the LFT program is vulnerability (that is, kill given a hit).

(1) Susceptibility is the degree to which a weapon system is open to effective attack due to one or more inherent weakness. Susceptibility is a function of operational tactics, countermeasures, and probability of enemy fielding a threat.

(2) Vulnerability is the characteristic of a system that causes it to suffer a definite degradation (for example, loss or reduction of capability to perform its designated mission) as a result of having been subjected to a certain (that is, defined) level of effects in an unnatural (that is, manmade) hostile environment.

c. Recoverability is the ability to take emergency action, following combat damage, to prevent loss of the system, to reduce personnel casualties, or to regain weapon system combat mission capabilities.

d. Lethality is the ability of a munition or directed energy weapon to cause damage that will cause the loss or a degradation in the ability of a target system to complete its designated missions.

e. Covered System is a major system that is user-occupied and designed to provide some degree of protection to its occupants in combat, or a conventional munitions program or missile program. Included as covered systems are conventional munitions programs for which more than one million rounds are planned for acquisition and a modification to a covered system that is likely to affect significantly its survivability or lethality.

f. Building-block approach is a strategy for vulnerability/lethality testing that generally begins with component level testing and progresses through sub-system, ballistic hull and turret, system level testing, and culminates in a FUSL LFT.

S–3. Live fire test detailed test plan

The LFT DTP provides explicit instructions for the conduct of the LFT. (See para 6–29.) It is prepared by the live fire tester and is derived from and implements the test conditions and data requirements in the EDP. The format and content of the LFT DTP can vary depending on the nature of the individual LFT (for example, component LFT, subsystem level LFT, or FUSL LFT). As a minimum, the DTP for a FUSL LFT should contain individual sections that address the major categories listed below:

a. Cover page. The cover page provides the name of the system, the activity or agency responsible for preparation of the plan, the date, plan classification, and applicable distribution statements.

b. Coordination sheet. The coordination sheet contains the signature of Army and DOT&E approval authorities.

c. Administrative information. A page providing administrative information on the position, name, organization, telephone number, and electronic mail addresses of key LFT&E personnel.

d. Introduction. The introduction contains a summary description of the test program, the principal participants and their roles, the test item (system) description, the test objectives, and any other information that supports LFT.

e. Test conduct. This section covers how the test will be conducted; which threats or targets are being used; what surrogates, if any, will be used; what procedures will be used to ensure test discipline; how threats will be fired/launched; and what potential lack of realism may result from the absence of components, from use of surrogate components, from the inerting of fuzes on stowed ammunition, and so forth. A tabular listing of all threats/munitions to be fired and target impact conditions or locations will be provided via summary tables; pictorial representations of each target impact location and attack angle will also be provided. Finally, the procedures to be used for the crew casualty and system damage assessments will be described.

f. Additional information. Additional information will be integrated into the body of the DTP or provided as individual appendices to address subjects such as the following:

(1) *System configuration.* This information, which requires input from the system PM, describes the system configuration and its fidelity (that is, how the test item compares to the production item that is expected to be fielded). All stowage plans for full-up targets will be pictorially presented to show locations and quantity of items stowed onboard as configured for combat. These stowage plans will be approved by the combat user for U.S. systems and by the intelligence community for foreign systems, before they are incorporated into the LFT DTP.

(2) *Instrumentation plan.* The instrumentation plan describes the instrumentation suite required to record test conditions and measure system response (for example, projectile striking velocity, fuel temperature, and component acceleration). The tester will define specific instrumentation requirements based on the SEP/EDP data requirements.

(3) *The operational security plan.* This plan is included as part of the DTP to ensure that all test participants are aware of the security aspects of the LFT and how the data are to be handled. Furthermore, the high visibility and sometimes controversial nature of LFT requires strict compliance with operations security safeguards.

S–4. Live fire test detailed test plan preparation and approval

The LFT&E plans matrix in the LFT&E strategy identifies which LFT requires a DTP to be submitted to DOT&E for approval or for review and comment. For building-block approach LFTs that do not require DOT&E approval, the DTPs will be approved by the test agency. Coordination and approval of those DTPs will be accomplished in accordance with existing Army T&E policy, and the test agency will forward copies of those DTPs to HQDA for the DUSA (OR) submittal to DOT&E. The DTP is prepared by the live fire tester and coordinated with members of the LFT&E working group. Two copies of the DTP (along with two copies each of the previously approved SEP and EDP and SLAD's Pre-Shot Prediction Report) are forwarded to the DUSA (OR) at least 60 days before test initiation. The DTP is either approved for the Army by the DUSA (OR) or returned to the tester for changes or corrections. Once approved by the DUSA (OR), the DTP is forwarded to DOT&E for review or approval, as required. Testing will not start until the DTP is approved by the DUSA (OR) and OSD DOT&E.

S–5. Live fire test detailed test plan change procedures

a. For those LFTs not requiring DUSA (OR)/DOT&E approval of the DTP, changes to the DTP are coordinated and approved via existing Army T&E policy (see AR 73–1).

b. For LFTs requiring HQDA (DUSA (OR) or OSD DOT&E approval of the DTP, as identified in the TEMP, generally FUSL LFTs, the DTP must outline the detailed procedures to be followed to accommodate unexpected changes to the LFT that may occur during actual testing. When a change to the approved DTP is required, it is essential that strict adherence to the change procedures be followed to avoid repeating test shots and to dispel any perceptions of "fixing" the test to achieve desired results. The tester takes the lead in coordinating changes to the DTP and ensures these changes are fully coordinated with all participating LFT&E agencies. Written notification of the proposed changes is forwarded through the DUSA (OR) to DOT&E for approval. No change from the DTP is undertaken until approved by the DUSA (OR) and DOT&E. After DOT&E approval, all participating agencies are notified of the change approval. The change will also be documented in the final test report along with the supporting rationale that is derived from an approved change to the LFT EDP if the change was required as a result of a test design change.

S–6. Live fire test battlefield damage assessment and repair support plan

The BDAR support plan is prepared by the U.S. Army Ordnance Center and School for FUSL LFTs on ground combat vehicle combat systems and by the U.S. Army Aviation Logistics School for FUSL on aviation systems and defines the level of BDAR to be performed. It describes team membership, repair skill level requirements, and times for repair. The support required by the BDAR team will be decided on a test by test basis in coordination with ATEC's AEC depending on the fidelity of the target. Typically, BDAR teams perform operator/crew, unit, and/or direct support

(DS) forward levels of BDAR repairs. The BDAR support plan will be submitted to HQDA (DUSA (OR)) and OSD DOT&E for approval along with the EDP and DTP for the FUSL LFT and provided to ATEC for information.

S–7. Live fire test conduct

The following provides general guidance for the conduct of FUSL LFTs and discusses those parameters and functions that must be considered during test planning (for example, vehicle stowage, instrumentation, and scheduling). Actual test requirements will be established on a case-by-case basis to address the data requirements defined in the SEP/EDP. Guidance presented in this chapter is based on Army LFT&E experience to date. Test conduct, test parameters/functions, and the terminology reflect this experience. Because one primary purpose of LFT&E is to address crew survivability, most of the parameters/functions and the testing discussed in this chapter is applicable to any type of system and the remaining items are easily applied to other types of systems. Again, the reader is cautioned that all requirements must be determined on a case-by-case basis.

a. FUSL Vulnerability LFTs are conducted to identify potential system integration vulnerabilities that cannot be adequately addressed through component and/or sub-system testing. In order to provide the most realistic test possible and to accurately assess the vulnerability of the system and the survivability of the crew, the weapon system must be as close to its combat configuration as possible. Combat configuration denotes a combat configured, fully functional item complete with all sub-systems and on-board stowage items.

(1) The presence of a combat configured, fully functional item with all sub-systems is particularly important in evaluating ballistic damage and the interaction between sub-systems as a result of damage to different components. In order to determine the individual effects of each shot on the test item, the test item is repaired and system functionality is baselined before each test shot. Baseline procedures should include a complete functional check of all major subsystems on the test item and may also include performance checks for parameters such as engine output.

(2) Systems undergoing LFT are stowed in a combat configuration so that the effects of the stowage on the system vulnerability and crew survivability can be assessed. Stowage in a combat configuration includes ammunition, fuel, additional authorized list (AAL) items, and basic issue items (BII). Anthropomorphic simulants and/or wooden mannequins are located in crew positions as an aid in crew survivability assessments. Ammunition should be live, with inert fuzes or fuzes removed (live fuzes damaged during test conduct could present a hazard to test personnel). However, if the reaction correlation between inert and live ammunition is known and predictable, inert munitions may be stowed to ensure survivability of limited assets (for example, to avoid the premature loss of test items before all the test shots can be completed). The use of inert ammunition instead of live ammunition will be approved via the EDP/DTP approval process on a case-by-case basis. Any planned shot that the PM considers to be catastrophic or of significant damage may be conceded; however, conceded shots will be assigned a Probability of Kill (Pk) = 1.0 for the evaluation.

(3) All fuel in the test item will be at normal operating temperatures for the system at the time of the test firing. This is necessary since the flammability of the fuel increases as its temperature increases.

(4) The AAL and BII are stowed on the test item in accordance with an approved stowage plan. The stowage plan is developed by the responsible TRADOC school and verified by the tester before testing. Crew simulants are dressed in the appropriate ensemble to include helmet, personal weapons, goggles, gloves, boots, coveralls, ballistic vest, and battle dress uniform, as prescribed by Army doctrine. This ensures that the anthropomorphic simulant or wooden mannequin is representative of an actual crew member and that the protective features of the uniform are accounted for in the crew injury evaluation.

(5) A hazard analysis is performed on all of the stowage items. Any stowage item that could pose a hazard to test personnel, if damaged during testing, must be modified or replaced. Those items modified or replaced must be listed in the EDP/DTP. For example, certain types of chemical detectors used on combat vehicles contain a radioactive isotope as part of the sensor. This isotope would be removed before stowing the detector to avoid contamination of the test site and potential hazard to testers.

b. The focus of FUSL live fire lethality tests is to demonstrate the effectiveness of U.S. munitions against representative threat targets. However, the test approach is somewhat different than that for vulnerability tests. Although it is desirable to configure the threat system target in a full combat configuration (that is, fully operational and stowed per an approved stowage plan), the target condition, system repair capability, and repair parts availability may require acceptance of some limitations. The FUSL live fire lethality tests generally provide a mechanism for evaluating munition effectiveness against realistic targets based on the contributions of principal damage mechanisms such as penetration/perforation and spall. However, in order to avoid a premature loss of a threat target, it may be necessary to minimize the potential for an early loss of the target from fire by minimizing the use of fuel and munitions/combustibles on the threat target. This may result in accepting some limitations with regard to assessing the contributions of fire, blast overpressure and toxic fumes on system loss of function and crew casualties. The use of inert ammunition

in lethality LFT&E targets may be prudent since it is important to investigate the contribution of the primary damage mechanisms to system damage in a limited number of shots and impacts into stowed ammunition may represent only a limited number of likely shot lines.

S–8. Live fire test resources

The full-up system level LFT is normally the last test to be conducted before the FRP DR and, as such, planning and resourcing must be addressed early-on in the LFT&E program. The strategy and resource requirements (to include targets/munitions, and an overview of On-Vehicle Equipment/BII and spare/repair parts) to accomplish an efficient and effective LFT&E program to include building block approach tests must be included in the TEMP T&E Resource Section (that is, Part V).

S–9. Live fire test schedule

Conduct of the FUSL LFT is driven by the time required between shots to repair the target. Full-up system tests, especially vulnerability tests, may require extensive repairs and repair time. Experience indicates that there is roughly a three-to-one ratio of repair time to test range time. To increase test efficiency and provide maximum utilization of personnel and hardware, it is advantageous to conduct LFTs with multiple target assets. Multiple target assets allow for overlapping of test and repair time, thus, increasing testing efficiency. When multiple test assets are not feasible, the LFT&E schedule must reflect the total time estimated to complete the testing to include repair times. If the schedule cannot accommodate these time requirements, it may be necessary to restructure the strategy. Decisions concerning assets, schedules, and strategy are addressed by the LFT&E working group and reflected in the LFT&E strategy. As with other phases of the T&E process, unresolved issues are forwarded to higher headquarters for resolution.

S–10. Live fire test instrumentation

A complete set of data must be gathered on each shot to facilitate the crew casualty and system damage assessment, to measure and/or record test conditions, and to ensure test conformity (that is, compliance with the EDP/DTP). In addition to instrumentation for addressing crew casualties and system damage, the test item is generally instrumented to provide early warning of potential problems resulting from the test event. Parameters measured could include engine RPM, voltage, hydraulic fluid pressures and temperatures, oil pressures and temperatures, coolant temperatures, and automatic fire suppression/fire extinguishing system discharges. Actual instrumentation suites are determined by the tester on a case-by-case basis to address the SEP/EDP/DTP data requirements and test item safety/security requirements. These instrumentation packages typically include the following for FUSL Vulnerability LFTs:

a. Video and high-speed photography to provide visual documentation of the test event. Video documentation provides real time monitoring of the interior and exterior of the test item. The exterior video also assists in locating parts displaced by the munition/target interaction. The internal video provides real-time information on perforation of the target protective system, the presence and extent of internal fires, and test item status information required for determining when it is safe for test personnel to re-enter the test site.

b. Projectile flight/performance instrumentation to record striking velocity, pitch/yaw at impact for dynamically fired munitions, and warhead timing data as appropriate (for example, tandem warheads). Video cameras, high speed cameras, and/or flash x-rays (FXRs) may be used.

c. Toxic fumes instrumentation to record the levels of potentially hazardous gases (for example, nitric oxide, nitrogen dioxide, carbon monoxide, carbon dioxide, hydrogen fluoride, hydrogen bromide, cyanide, and aldehydes) and airborne particulates. Toxic fume data are collected at crew member locations. Specific items and crew locations to be sampled are system dependent and will be determined based on an analysis of the potential hazard posed by onboard materials.

d. Thermal effects instrumentation to record temperature and heat flux data related to the crew and test item. These data are used to assess crew survivability, provide engineering data to assess hardware vulnerability, and ensure compliance with the EDP/DTP parameters (for example, fuel temperature at shot time).

e. Blast overpressure instrumentation to record pressure time histories. Overpressure data are collected in the crew compartment and external to the test item to assist in assessing personnel casualties and to provide engineering data to assess hardware vulnerability.

f. Ballistic shock instrumentation to record accelerations and forces on the crew and critical system components. Accelerometers, strain gages, or velocity gages can be placed on components to measure the ballistic shock transmitted through the structure of the test item to the components, and on anthropomorphic simulants, where appropriate, to measure acceleration and forces transmitted to the crew. When used, instrumented anthropomorphic simulants are positioned in crew locations away from the primary penetrator path/spall cone to avoid destruction of expensive test

equipment and the loss of test data. Wooden mannequins can be placed in other crew locations to record the effect of the penetrator/spall cone.

S–11. Live fire test facilities

Live fire testing often requires extensive test facility capabilities to allow for realistic and cost effective testing. Actual facilities for a given program will be driven by the test and data requirements. Test facility capabilities that could be required to support a given program are as follows:

a. Multimunition firing. The threat could consist of gun fired projectiles, missiles, rockets, and mines requiring a variety of launching or firing capabilities. Threats could require real range firings, reduced range firings, and static firings (for example, mine firings in prepared soil with specified density and moisture content). Launch conditions could be direct fire, super-elevation (that is, anti-air simulation), or high angle of fall (that is, indirect fire simulation).

b. Instrumentation suite. FUSL live fire testing may be instrumentation intensive and could require upwards of 200 channels of data collection during any given shot. Substantial video and high-speed film coverage for documentation and test item security could be required.

c. Range/test item security. In addition to video to provide real-time visual security, an auxiliary fire suppression system could be required to protect range and instrumentation suite facilities as well as test item security. Providing adequate protection to instrumentation cables from fragments or fire to ensure test requirements are not compromised must be a prime consideration. Additionally, environmental protection in accordance with Federal and State government mandates must be adequately addressed. EISs must be developed, staffed, and approved before test initiation.

d. Repair facility. Because test assets are limited and FUSL LFT&E test item or target configuration requirements are stringent, the ability to perform repairs will be necessary. These repairs could include welding, machining, fabricating or replacing damaged components, and major reconstruction of the test item. Repair up to depot level could be required.

S–12. Test discipline for full-up, system-level live fire test

The high-visibility and oversight of LFT requires strict discipline during the conduct of the testing. LFT phases other than the FUSL LFT will generally be managed and executed in accordance with existing Army T&E policy (see AR 73–1) unless specific LFT considerations warrant otherwise and are reflected in applicable test planning documentation.

a. Adherence to the detailed test plan. One of the primary responsibilities of the tester is to ensure that the test is conducted in accordance with the HQDA or DOT&E-approved DTP. Unauthorized deviations from the DTP are not permitted. Additionally, the LFT will not start until the DTP are approved. With FUSL LFTs generally scheduled near the critical FRP DR and test shots relatively expensive, it is essential that the DTP be followed to avoid potential problems. Conducting the test according to an approved DTP will eliminate the perception of bias or of rigging the test in order to ensure positive results. Changing shotlines, threats, and stowage even for sound technical reasons, without proper coordination and authorization, is not permitted.

b. Change procedures. A LFT is rarely conducted without some deviation from the approved DTP being required. To address these potential deviations and retain testing integrity, a strict procedure has been adopted for approving changes to the DTP as described in paragraph S–5.

c. Reporting emerging results. The dissemination of emerging results provides test participants a continuing awareness of test progress and an early identification of potential vulnerability/lethality shortcomings. Damage assessment meetings that are scheduled and moderated by the damage assessment team (DAT) chair should be held periodically throughout the test so that data can be reviewed, commented on, and necessary subjective judgments reviewed for consistency and soundness. Representatives of the DAT, PM, and system contractor are typically present at these meetings. However, it should be noted that in assessing the shots, the PM and system contractor are present to provide information on system design characteristics, if required. The DOT&E will have access to these meetings; however, any results addressed during these meetings and used in the DOT&E assessment report will be provided to the Army for factual review before its use. Emerging data from the DAT, generally in the form of summary charts incorporating results of deliberations during the damage assessment meeting, will be marked to indicate that the data are draft or in preliminary form. Emerging results and all finalized damage assessment data will be released by the DAT to the tester and system evaluator for use and secondary distribution as required by T&E protocols.

S–13. Damage assessment team for full-up, system-level live fire test

After each shot, the target is examined and the system damage and crew casualties are assessed. This section defines the Army approach to this process. The DAT is the team that collects and assesses crew incapacitation and/or test item/target damage after each shot. The DAT is chaired by SLAD and will include the tester (for all tests) and the user

(for vulnerability tests only) as members. The DAT will consult with other organizations as needed for technical expertise or input. All such subject matter experts will be acknowledged in emerging and final damage assessment results. The specific tasks of the DAT are to—

a. Document any physical damage to the simulated crew members and assess the extent of their injuries (that is, level of incapacitation).

b. Document any physical damage to the test/target item.

c. Determine if any injury, degradation, and/or loss of system capability occurred that would affect the ability of the crew and system to perform their mission.

d. Determine the damage mechanisms causing any injury, degradation, or loss of function.

e. Characterize the test item's performance and other parameters, before and after each shot, to allow for future vulnerability reduction/lethality enhancements.

f. Document and characterize behind-armor effects produced by the test munition.

g. Use the preceding information to assess crew casualties and determine system loss of function or degraded combat utility for the test munition.

h. Document the final damage assessment for each shot. Necessary subjective judgments will be based upon the majority viewpoint of the DAT. The damage assessment results for each shot are documented in the Final Test Report prepared for the LFT.

S–14. Crew vulnerability for full-up, system-level and system level live fire tests, when appropriate

Crew vulnerability can be assessed by examining data collected with crew simulants and crew environment instrumentation.

a. Crew simulants can be used to support an assessment of expected incapacitation of crewmembers. The following simulants have been used in previous LFTs:

(1) Fully combat dressed wooden mannequins placed in crew positions in the expected penetrator path/spall cone where acceleration injury is not a main concern. After each shot, the fully combat dressed mannequins are assessed for damage (for example, burns on clothing, damaged body parts, fragment penetration/perforation, and similar changes).

(2) Fully combat dressed anthropomorphic simulants (that is, "anthros") placed in crew positions where acceleration is the main concern. "Anthros" can be used to measure triaxial acceleration, compression, biaxial bending, fore-aft bending, and neck shear.

b. The crew compartments can be instrumented to collect thermal, toxic fumes, and blast overpressure data. The following crew environmental data have been collected in previous LFTs:

(1) Temperature and heat flux levels at each crew member location. These data allow a determination of the level of burn damage and the effectiveness of the crew member's protective uniform.

(2) Toxic fumes levels at each crew member location. Data on toxic gases, pyrolysis products, and airborne particulates are collected.

(3) Blast overpressure levels at each crew member location. These data are used to determine the level of crew incapacitation due to injury to the air containing structures of the body (for example, lungs and ears).

c. The collected crew simulant and environmental data are analyzed and compared to approved crew injury criteria to determine an expected level of crew incapacitation. These data are used by SLAD in the overall crew survivability assessment.

S–15. Vehicle vulnerability for full-up, system-level (and system level live fire tests, when appropriate)

After each individual shot, all damage is recorded, as well as obvious vehicle functional degradation (that is, engine will not run). This damage assessment is then used to determine vehicle vulnerability in the form of system loss of function or degraded combat utility. These estimates are derived through the use of fault-tree or deactivation diagrams. Specific kill criteria to be used will be determined by the DAT chair and the system evaluator for each specific LFT program.

a. In addition to providing insights into system vulnerability, LFT&E programs can provide the Soldier hands-on experience in BDAR. BDAR efforts conducted in conjunction with FUSL LFTs can provide the user insights into the time, parts, tools, and skills required to repair the system or to upgrade a damaged system to a combat-capable condition. Evaluation of a system's capabilities immediately following a simulated threat attack compared to the system's capabilities following operator/crew, unit, and DS BDAR provides insights into the effectiveness of BDAR techniques, tools, and training.

b. Another aspect of the LFT&E process is to examine the spare part supply line to ensure that parts stocked are in fact those required to support damage sustained from a battlefield encounter.

S–16. Final test report for full-up, system-level live fire tests

The final test report, prepared by the tester/DAT, provides a formal detailed record of the test data and information obtained during the conduct of the LFT, and describes the conditions that actually prevailed during test execution and data collection. The test report documents all individual shot test conditions and test results required by and identified in the DTP and approved changes to the DTP. The final test report is provided to the DUSA (OR) for approval 60 days after test completion, as well as to the system evaluator. The approved final test report and SER must be forwarded to DOT&E within 120 days after test completion and 45 days before the FRP DR. Schedules must be planned accordingly to accommodate these mandatory reporting milestones.

Appendix T

Software Testing

T–1. Overview of software testing

This appendix briefly describes a variety of software testing methods that can be used to detect errors, develop sets of test data, and monitor computer system resources. These methods serve only as a representative sample, rather than an all-inclusive list. See appendix Q, which also addresses DT of software.

T–2. Software test limitations

a. The objective of functional or "path" testing is to use known input data to check whether the output functions meet established specifications. Each piece of input data will generate a software function along a specific path of digital logic. However, the technology of real-time, embedded software places strict limitations on the number of software elements that can actually be exercised in a functional test.

b. The most significant technical difficulty in path testing is to create test cases that will provide adequate coverage of the software paths. Success of path testing is determined by the degree of coverage that is achieved. However, many test data sets will produce either redundant paths or paths that are infeasible because they violate design constructs of the software. Therefore, selecting an adequate set of test cases requires specialized support tools, even for non-complex programs.

c. The difficulty in achieving adequate test coverage also prohibits use of a single, OT to certify software acceptance. Most embedded software programs are large, containing many modules and decision statements that may produce different outputs with the same inputs but with slight variations in execution times. Identifying the actual source of an error in an OT is extremely difficult.

d. A longer test is also no guarantee of adequate coverage, due to unequal distribution of modular run times. Most disciplined software development processes use a modular, hierarchical approach to design and test software. Top-level modules provide functional control over the lower-level modules that they call for. Therefore, the top-level software modules are exercised much more frequently during integration testing than the lower-level modules that await calls. Various estimates of run-time distributions have documented that only 4 to 10 percent of software architecture will operate for 50 to 90 percent of the total run time. Therefore, increasing the length of a test may only fractionally expand coverage of software functions.

T–3. Software incremental testing

An incremental test strategy allows a variety of test events that are diverse enough to provide confidence in the effectiveness of the test process. In addition, an incremental strategy provides a means to identify and correct failures earlier and more effectively. Specific test events and levels are tailored to the needs of each system acquisition.

T–4. Software testing techniques

Testing takes place at various points of the software development process that are generally common to all software projects. They are—

a. Unit testing in which each unit, or basic component, of the software is informally tested to verify that the detailed design for the unit has been correctly implemented. Unit testing validates each program unit in isolation. The tests are usually performed by the programmer who designed and coded the unit.

b. Software integration testing in which progressively larger groups of tested software units are integrated and tested until the software works as a whole.

c. System testing in which the software is integrated with the overall product and tested to verify that the system meets its specified requirements.

d. Acceptance testing generally involves a subset of system tests that formally demonstrates key functionality for final approval and contract compliance. Acceptance testing is witnessed by the customers; it may be performed at the developer's site or at the user's site. Each of these four test stages make use of static and dynamic analysis techniques that are described in paragraphs T–5 and T–6.

T–5. Static software analysis

Static analysis examines or analyzes a software product without executing the code on computer or system hardware. Instead, static analysis is a manual task or an automated process using static, source code analysis tools. Static analysis tools can demonstrate the absence of certain types of defects, such as variable typing errors, but they cannot alone

detect faults that depend on the underlying operating environment. Consequently, effective software testing requires a combination of static and dynamic analysis approaches. Static analysis techniques include the following:

a. Reviews, walk-throughs, and code inspections examine design and technical documentation to detect errors. The procedure typically involves a small working group of programmers and technical personnel who assess requirements documents, design specifications, and program listings. This static analysis procedure is an essential task in software development. It is commonly referred to as peer review, which is one of the KPA that a developer must perform to achieve level 3 through 5 in the Capability Maturity Model (CMM). Peer review may include an individual or group analysis of design logic representations, a line-by-line code reading, analysis of documentation on test inputs, or tracing requirements from document to document.

b. Code audits examine the source code to determine whether prescribed programming standards and practices have been followed.

c. Interface checking examines the flow of information and control within a system to identify areas where mistakes can occur, such as calling the wrong procedure or passing the incorrect data.

d. Physical units checking specify and checks measurement units in computations.

e. Data flow analysis detects whether or not sequential events occur in software execution.

f. Structure analysis detects violations of control flow standards, such as improper calls to routines, infinite loops, and incidents of recursion in design products or source code.

g. Cross reference checking produces lists of data names and statement labels to show all places they are used in a program.

h. Input space partitioning uses path and domain analysis, or partitions to build sets of test data that cause a selected path in software to be executed.

i. Complexity analysis examines algorithm design or coded programs to examine the density of decision options, number of operations required, amount of capacity used, or understandability of the code.

T–6. Dynamic software analysis

a. Dynamic analysis executes the software to determine if it functions as expected. Dynamic analysis may involve running the software in a special test environment with stubs, drivers, simulators, test data, or it may use an actual operating environment with real data and operational conditions. Current tools attempt to detect faults rather than demonstrate their absence. Additionally, most of these tools can only detect faults that extend to software outputs, unless the software has been specially instrumented to monitor internal data elements (intrusive monitoring) or special hardware monitors have been attached to the system (non-intrusive monitoring). Most importantly, the effectiveness of any dynamic analysis technique is directly related to the quality of the test data.

b. Proper selection of input data must be based on an accurate description of the design of the computer program and host system. In most large-scale, software development programs, accurate design information may be best derived through the V&V effort. The objective of software V&V prior to functional testing is to ensure that the software design conforms to established specifications and that the design and code are free of errors. Software must conform to requirements specifications at each level of the system to allow proper assessment of system outputs. Software functions can be verified as correct only if the observed system output is in compliance with the intent of the test case input. Specifications must be written with a level of detail to allow verification of proper input/output relationships at every level in the system. The V&V process will also provide the technical insight to program design and behavior that is required to structure an effective stress test program.

c. Dynamic analysis techniques include the following:

(1) Functional (black box) testing is the most commonly used dynamic analysis approach. This approach executes the program with specific, controlled input to verify that the program performs the correct functions. For functional strategies, test data are derived from program requirements without regard to program structure. The amount of software that can be exercised in a functional test is limited by the test environment and the time available for testing. Therefore, use of this method alone does not guarantee a thorough test of the software source code or an absence of errors.

(2) Structural (white box) testing requires knowledge of the source code, including program structure, variables, or both. In structural strategies, test data are derived from the software program's structure. This approach executes the software program with specific, controlled inputs to provide a degree of coverage for the control paths, data paths, and conditions within the software program.

(3) Real-time testing, or stress testing is performed to ensure that software will support the system under the stress levels that are expected in the actual operating environments. These tests are often structured to go beyond the expected conditions to determine points where the software operation will cause system failure. Test configurations that may be used in structuring a software stress test are as follows:

(a) Excessive system functional loads that are required to support tactical operations.

(b) Extreme software inputs or conditions that cause extreme outputs.

(c) "Illegal" data inputs or conditions that replicate operator-induced input errors or equipment errors under field stress.

(d) High loading of computer capacities, including storage and processing utilization.

(4) Assertion testing uses an assertion preprocessing tool to specify and assess the intent of input, output, intermediate steps of functions, and constraints.

(5) Model-based testing is used to systematically select a set of test case inputs and outputs that have a high probability of detecting existing errors.

(6) Performance measurement techniques monitor software execution to locate code or throughput inefficiencies, either by random sampling or by means of software probes.

(7) Path and structural analysis monitors the number of times a specific portion of code is executed, the amounts of time involved, and other design parameters to detect errors in computation, logic, data handling, or output.

(8) Interactive debugging techniques control program execution and analyze any part of a program while it executes.

(9) Random testing can reveal unexpected program behavior by executing the program with random data and comparing the actual output to the expected output.

(10) Mutation analysis studies the behavior of many versions of the same program that have been mutated with a number of errors to check that each mutant produces different output data when given the same input data.

(11) Error seeding uses the percentage of detected errors to extrapolate the estimated number of remaining errors in a large software system.

T–7. Security certification

The software test program must accommodate the requirements of AR 25–2 regarding information security. Examining the control of the procedures used during design and test to develop software is an integral part of the software certification and system accreditation process.

a. Software must be completely tested before becoming operational.

b. Both valid and invalid data must be used for testing.

c. Testing is not complete until all security mechanisms have been examined and expected results attained.

d. Upon completion of maintenance or modification of software, independent testing and verification of the changes is required before returning the software to operation.

T–8. Computer software configuration item qualification testing

a. During this activity, the developer prepares and demonstrates all the test cases necessary to ensure compliance with the CSCI software and interface requirements.

b. If a multiple build software acquisition strategy is in effect, this activity for a CSCI is not complete until that CSCI's final build, or possibly later builds involving items with which the CSCI is required to interface.

c. Historical equivalent activities are—

(1) CSCI formal qualification test.

(2) Materiel system computer resources.

(3) Software development test cycle/system testing (partial).

(4) AIS.

d. The objective of CSCI qualification testing is to demonstrate to the acquirer the CSCI's ability to meet its requirements as specified in its software and interface requirements specifications.

e. Entry criteria can consist of—

(1) The CSCI should successfully complete unit integration and testing, including developer internal CSCI testing.

(2) Test preparation effort, including STD preparation and dry run, should occur prior to running a formal test witnessed by the acquirer.

f. Test activities include—

(1) The developer establishes test preparations, test cases, test procedures, and test data for CSCI qualification testing and records this information in the appropriate STD.

(2) Benchmark test files are used as test data, if available.

(3) Prior to an acquirer witnessed test, the developer should perform a dry run of the test in accordance with the test cases, procedures and data in the STD. The results are recorded in the appropriate software development files and test cases or procedures are updated as needed.

(4) The developer conducts CSCI qualification testing in accordance with the test cases, procedures, and data in the STD.

(5) All discrepancies, malfunctions and errors will be documented in problem and change reports and entered into the developer's corrective action system.

(6) Results of CSCI qualification testing are recorded in a STR.

(7) Test results are analyzed, software revised and retested at all necessary levels, and the software development files and other software products updated based on the results. The acquirer should be notified in advance when qualification retesting is to occur.

(8) The operating environment for CSCI qualification testing is usually a local test bed system. However, qualification on target or production representative system is preferred, particularly for embedded materiel system computer resources.

g. Evaluation activities are as follows:

(1) CE activities include—

(a) Review of the STD to ensure CSCI qualification test preparations, test cases and test procedures are adequate to verify compliance with software test plan and SRS and interface requirements specification requirements.

(b) Assessment of test drivers for their ability to induce data and processing loads stated in the OMS/MP. See AR 71–9 for details on the OMS/MP.

(c) Ensuring traceability from each STD test case to its CSCI and software interface requirements and, conversely, from each CSCI and applicable software interface requirement to the test cases that address it.

(2) Implementation and analysis of applicable metrics.

(3) If needed to resolve open issues or address areas of risk identified in the evaluation process, a formal TRR is appropriate.

h. The metrics marked with an X in table T–1 apply to CSCI qualification testing.

i. Representative products, documents and decision criteria typically addressed during CSCI qualification testing are shown in table T–2. Items marked "final" should contain comprehensive material that corresponds to the current build and level of qualification testing.

Table T–1
Metrics applicable to computer software configuration item qualification testing

Applies	Metric
X	Cost
X	Schedule
X	Computer resource utilization
	Software engineering environment
X	Requirements traceability
X	Requirements stability
X	Design stability
	Complexity
X	Breadth of testing
X	Depth of testing
X	Fault profiles
	Reliability

Table T–2
Computer software configuration item qualification testing decision criteria—Continued

Primary responsibility	Principal products affected	Decision criteria
PM and developer with software quality assurance and IV&V	TRRs, if required, to resolve open issues	Ready to perform CSCI qualification tests
S/W developer	STD STD STR	Draft Dry run of CSCI qual. test in accordance with STD Final Final
S/W developer and Government software quality assurance or IV&V	Requirements traces Metrics reports	Updated Acceptable degrees of requirements traceability and stability; CRU; design stability; breadth and depth of testing; fault profiles

Appendix U

Test and Evaluation Documentation Overview

U–1. Documents summary

Table U–1 summarizes the T&E documents, to include related documents.

U–2. Document formats

Specific formats for the T&E documents will be made available upon request by contacting the proponency office for this document (TEMA (703) 695–8995/8999, DSN 225).

Table U–1
Test and evaluation documents

Document	Reference	Responsible agency	Summary
Detailed test plan (DTP)	AR 73–1	Test organization	The DTP is an event-level document used to supplement the EDP by providing explicit instructions for the day-to-day conduct of a test. It is derived from and implements the SEP, and governs test control, data collection, data analysis, and the necessary administrative aspects of the test program. There may be one or several DTPs, depending on the complexity of the program and the number of test sites or test facilities providing data. The DTP is coordinated with the system evaluator and with other T&E WIPT members, if necessary, to ensure that it accurately and completely reflects the requirements for data, information, and analysis set forth in the EDP (if available). DTPs for FUSL LFT&E are submitted through the DUSA (OR) to the DOT&E for approval. See appendix S for LFT DTP information.
Developmental test readiness statement (DTRS)	AR 73–1	Materiel developer	The DTRS is a written statement prepared by the chair of the DTRR as part of the minutes. The statement documents that the materiel system is ready for the PQT or the IT system is ready for the SQT. See chapter 6.
Doctrine and organization test support package (D&O TSP)	DA Pam 73–1	TRADOC (combat developer)	The D&O TSP is a set of documentation prepared or revised by the CBTDEV or FP for each OT supporting an acquisition milestone decision. Major components of the D&O TSP are means of

Table U–1
Test and evaluation documents—Continued

			employment, organization, logistics concepts, OMS/MP, and test setting. See paragraph 6–59 and figure 6–8.
Emerging results brief (ERB)	Defense Acquisition Guidebook and DA Pam 73–1	System evaluator	The ERB provides emerging evaluation results to members of the acquisition team and decisionmakers. It is prepared on a case-by-case basis but usually when information is required immediately after a key event and the final SER will not be available to support acquisition DRs. See paragraph 5–26e for information.
Environmental assessment (EA)	AR 200–2	Materiel developer	The EA addresses new and continuing activities where the potential exists for measurable degradation of environmental quality. This document concludes with either a finding of no significant impact (FNSI) or a notice of intent (NOI) to prepare an EIS. The EA, FNSI, and NOI are for public disclosure.
Environmental impact statement (EIS)	AR 200–2	Materiel developer	The EIS is prepared if the EA shows that the system will impact the environment adversely or is controversial. It provides full disclosure to the public on all issues associated with a Federal action that has the potential to significantly impact the natural environment. If required, testing is performed to identify and quantify the environmental quality issues.
Event design plan (EDP)	AR 73–1	System evaluator, tester, or event executioner	The EDP documents the results of planning the test design methodology and the data collection, reduction, and reporting processes required for the specific event or combination of events. An event is any activity that produces data for evaluation purposes (that is, any test, model, simulation, experiment, demonstration, or data collection opportunities during a training exercise). The EDP contains detailed information on event design,

Table U–1
Test and evaluation documents—Continued

			methodology, scenarios, instrumentation, simulation and stimulation, data management, and all other requirements necessary to support the evaluation requirements stated in the SEP. EDPs for FUSL LFT&E are submitted through the DUSA (OR) to the DOT&E for approval.
Five-year test program (FYTP)	AR 73–1	ATEC	The FYTP is a compendium of prioritized, TSARC reviewed, and HQDA approved OTPs for a 5-year period. The document identifies validated requirements to support the Army T&E program. It is a tasking document for the current and budget years and provides test planning guidelines for the out-years. See AR 73–1 for additional information.
Health hazard assessment report (HHAR)	AR 40–10	CHPPM	The HHAR is the formal document used to identify potential health hazards that may be associated with the development, acquisition, operation, and maintenance of an Army system. It also provides recommendations for eliminating or controlling hazards. It is required for the development of the Safety Assessment Report and is one of the domain assessments prepared in support of the MANPRINT assessment process. An health hazard assessment is conducted by the Commander, CHPPM. Information from the HHAR is input to the System MANPRINT Management Plan. (See AR 602–2.) See AR 40–10 for content and format.
Human factors engineering (HFE) assessment	AR 602–1	AMC/ARL–HRED	The HFE assessment summarizes the HFE issues based on the results of HFE analyses, testing, and system evaluation. The T&E input should be in the HFE design, Soldier-machine interface, system safety, methodology, data, and reporting areas. See AR 602–2 for format

Table U–1
Test and evaluation documents—Continued

			information.
Human use review approval	AR 70–25 and OTSG Reg 15–2	Office of The Surgeon General	Human use review approval is a written document prepared by the Human Subjects Research and Review Board (HSRRB) containing recommendations for approval, disapproval or deferred to The Surgeon General for all research, developmental, test, and evaluation activities including clinical investigation involving human subjects. Test plans, protocols, together with any and all associated health hazard assessments, safety assessment reports, safety releases and test plans are required to be submitted to the HSRRB by the responsible test agency or activity for review and approval prior to test or investigation initiation.
Independent evaluation brief (IEB)	DoDI 5000.02 and DA Pam 73–1	System evaluator	The IEB summarizes the report submitted to the milestone DR body and contributes to recommendations by the review body to the decision maker as well as to management decisions by the review body. The IEB is prepared after drafting of the SAR and follows the same outline as the SER. See paragraph 5–26d for additional information.
Live fire T&E (LFT&E) strategy	Defense Acquisition Guidebook and AR 73–1	System evaluator and developmental tester	A LFT&E Strategy is developed in coordination with the T&E WIPT for each program designated for LFT&E and is approved by DOT&E. It should be detailed enough to project resource requirements, schedule major T&E efforts, and trigger long lead-time planning, procurement of threats or surrogates, and modeling. The LFT&E strategy includes a Plans Matrix identifying all tests, test schedules, issues to be addressed, and the planning documents proposed for submission to DOT&E. It is the foundation for the LFT&E section of Part IV of the

Table U–1
Test and evaluation documents—Continued

			TEMP. See chapters 5 and 6 for additional information.
Logistics demonstration (LD) plan	AR 700–127 and DA Pam 700–127	Materiel developer	The LD plan is developed with coordination of the Supportability and T&E WIPTs. The plan describes the details of how troubleshooting and repair procedures will be demonstrated. It provides details on logistic support resources provided for the demonstration, identification of the faults to be inserted, detailed procedures for conducting the demonstration, plans for collecting and analyzing resulting data, and any constraints or limitations. See chapter 11 of DA Pam 700–127 for format information.
Logistics demonstration (LD) report	AR 700–127 and DA Pam 700–127	Materiel developer or PM	The LD Report is developed in coordination with the Supportability WIPT and the T&E WIPT. The report documents results of the LD, including specific task results, supporting analysis, and comments from participants and data collectors. The LD Report is generally completed 45 days prior to the next DR. See DA Pam 700–127, chapter 11, for format information.
MANPRINT assessment	AR 602–2	DCS, G–1	The MANPRINT Assessment Report is the formal overall assessment of the analyses done in each of the seven MANPRINT domains: manpower, personnel, training, HFE, system safety, health hazards, and Soldier survivability. The draft MANPRINT assessment report is forwarded to DCS, G–1 for approval. See AR 602–2 for the format information.
Model Comparison Report	Defense Acquisition Guidebook	ARL (SLAD)/SMDC	The Model Comparison Report includes an in-depth comparison of the FUSL LFT pre-shot predictions of crew and system damage and the observed test outcomes. This report can contain damage assessment information that will be published in the test

Table U–1
Test and evaluation documents—Continued

			plan as well as additional data analysis.
New equipment training test support package (NET TSP)	AR 350–1	Materiel developer	A NET program is first prepared by the MATDEV to support training development for new materiel and IT systems, including conduct of T&E of new equipment and software. Based on the NET program, the MATDEV prepares, as appropriate, a NET TSP. The NET TSP is provided to the TNGDEVs and testers. It is used to train player personnel for DT and to conduct training of instructor and key personnel who train player personnel for OT. The TNGDEV uses the NET TSP to develop the training TSP. See paragraphs 6–55b and 6–58 and AR 350–1 for format information.
Operational test readiness statement (OTRS)	AR 73–1	Operational tester	The OTRS is a written statement prepared by the CBTDEV, MATDEV, TNGDEV or trainer, and test unit commander before the start of IOTs or FOTs for use during the OTRR. The OTRS addresses or certifies the readiness of the system for testing in each member's area of responsibility. An OTRS may be required for some FDT/E and should be specified in the OTP. See paragraph 6–46 and figure 6–7 for information on an OTRR.
Outline test plan (OTP)	AR 73–1	Test organization	The OTP is a formal resource document that identifies resources required to support an OT, FDT/E, or a DT requiring Soldier participants or other operational resources. The OTP is submitted to the TSARC for review and contains the test objectives, test conditions, scope, tactical context (OT or FDT/E only), resource requirement suspense dates, test milestone dates, and OT cost estimates for the specific test. See AR 73–1 for additional information.

Table U–1
Test and evaluation documents—Continued

Pre-shot prediction report	DA Pam 73–1	ARL (SLAD)/SMDC	The Pre-Shot Prediction Report provides the expected outcome (munition/target interaction) of each shot before actual test conduct and is required for all FUSL LFTs (or substitute test series). The report is submitted to the DUSA (OR) 60 days before test initiation. The Army approved Pre-Shot Prediction Report is then forwarded (with the DTP and EDP) to DOT&E for review and comment. See appendix S.
Record of environmental considerations	AR 200–2	Materiel developer	Briefly describes a proposed action and contains a checklist explaining why further analysis is not necessary. It is used when a categorical exclusion applies or there does exist environmental documentation on the item/system action.
Resume sheet	AR 73–1	Test organization	A Resume Sheet is a resource document that identifies resources required to support a CEP or any other TRADOC test requiring Soldier participants or other operational resources. The Resume Sheet is submitted to the Concept Experimentation Program Schedule and Review Council or TSARC for review and contains the test objectives, test conditions, scope, tactical context, resource requirement suspense dates, test milestone dates, and Customer Test cost estimates for the specific test. See AR 73–1 for additional information.
Safety assessment report	AR 385–10 and AR 40–10	Materiel developer	The Safety Assessment Report contains data and information relative to personnel and equipment hazards inherent in the system and any associated operation and maintenance hazards. Government system level testing cannot begin until the Safety Assessment Report is received, reviewed, and accepted by the test organization. See chapters 5 and 6

Table U–1
Test and evaluation documents—Continued

			and appendix N, system safety evaluation, and AR 385–10.
Safety confirmation	AR 385–10 and AR 73–1	ATEC (DTC)	The safety confirmation provides the safety findings and conclusions and states the hazards as Low, Medium, or High. It indicates if the item is safe for its intended use. The safety confirmation is appended to the SER. See paragraph 6–65, appendix N, and AR 385–10.
Safety release (SR)	AR 385–10 and AR 73–1	ATEC/Health Services Command/Medical Research and Development Command/U.S. Army Information Systems Command	The SR is required before any testing involving Soldiers begins. It documents the precautions that must be taken to avoid system damage and personal injury. The SR is based on the results of DT and data presented in the Safety Assessment Report. See paragraphs 6–63 and 6–64, appendix N, and AR 385–10.
System analysis report (SAR)	AR 73–1	System evaluator	The SAR provides the detailed analyses that support a SER and accounts for all issues and measures contained in the SEP. A SAR is also prepared to support a SA when the analysis is too detailed or inappropriate for inclusion in the SA and addresses only those issues and measures contained in the SA. See paragraph 6–61.
System assessment (SA)	AR 73–1	System evaluator	The SA provides an assessment of the progress toward achieving system requirements and resolution of issues. The scope of issues to be addressed by the SA is flexible. It may cover all or only some aspects of operational effectiveness, suitability, and survivability and may address technical aspects of a system. The SA is typically prepared as input to nonmilestone acquisition decisions or inquiries and to support system evaluation.
System evaluation plan (SEP)	DoDI 5000.02 and AR 73–1	System evaluator	The SEP documents the evaluation strategy and overall T/SES for the entire

Table U–1
Test and evaluation documents—Continued

			system acquisition life cycle. The SEP supports development of the TEMP by addressing the issues for testing, describing evaluation of issues that require data from sources other than tests, stating the COIC and CTPs, identifying data sources, providing the approach to the evaluation, and identifying program constraints. The SEP provides guidance for the development of EDPs and DTPs.
System evaluation report (SER)	DoDI 5000.02	System evaluator	The SER provides the independent evaluation of the system's operational effectiveness, suitability, and survivability. It is provided to the decisionmakers at each acquisition milestone reviews. It is based on test data, reports, studies, simulations, and other appropriate sources. It contains the evaluator's assessment of the technical parameters, conclusions, and position on the future capability of the system to fulfill the approved requirements and mission. The SER will contain an assessment of the adequacy of testing, the need for additional testing, and will identify program constraints and their impact on the evaluation. The safety confirmation is appended to the SER.
System MANPRINT management plan (SMMP)	AR 602–2	TRADOC	The SMMP is initiated by the CBTDEV or TNGDEV when the mission area analysis identifies a battlefield deficiency requiring development of new or improved materiel. The SMMP will be updated as needed throughout the materiel acquisition process. See AR 602–2 for format information.
System safety management plan (SSMP)	AR 385–10	Materiel developer or PM	The SSMP is a management plan that defines the system safety program requirements of the Government. It ensures the planning, implementation, and accomplishment of system safety tasks and

Table U–1
Test and evaluation documents—Continued

			activities are consistent with the overall program. requirements. See AR 385–10.
System safety program plan (SSPP)	AR 385–10	Materiel developer	The SSPP is a description of planned methods to be used by the contractor to implement the tailored requirements of MIL–STD–882, including organizational responsibilities, resources, method of accomplishment, milestones, depth of effort, and integration with other program engineering and management activities and related systems. See AR 385–10.
System safety risk assessment (SSRA)	AR 385–10	Materiel developer	The SSRA provides a comprehensive evaluation of the safety risk being assumed for the system under consideration at the milestone DR and supports the decision for accepting residual hazards. See AR 385–10.
System training plan (STRAP)	AR 350–1	Training developer	The STRAP reflects all training support required for both individual and collective training and for each MOS associated with the specific weapon or system.
System support package (SSP)	AR 700–127	Materiel developer	The SSP is a composite of the support resources planned for a system in the expected deployed environment. It consists of spare and repair parts, manuals, training package, special tools, test, measure, and diagnostic equipment, and unique software. The SSP is tested and validated during DT and OT and evaluated during the LD. The SSP will be delivered to the test site no later than 30 days before testing begins. See paragraph 6–57 and AR 700–127 for information and format.
System support package components list (SSPCL)	AR 700–127	Materiel developer	The SSPCL is a list of the components in the SSP that must be provided to the testing organization 60 days before testing begins. See AR 700–127 for additional information.

Table U–1
Test and evaluation documents—Continued

Test and evaluation master plan (TEMP)	DoDI 5000.02, Defense Acquisition Guidebook, and AR 73–1	Materiel developer or PM	The TEMP is the basic planning document for all T&E related to a particular system acquisition and is used by decision bodies in planning, reviewing, and approving T&E activities. It is developed in coordination with the T&E WIPT and must be approved or updated prior to each acquisition milestone. The TEMP addresses the T&E to be accomplished in each planned program phase. See chapter 3, TEMP 101 Brief, TEMA website, for format.
Test data report (TDR)	AR 73–1	Operational test organization	The TDR is a formal document that contains the test description, the actual test conditions, test limitations, deviations from the approved EDP, and the test team observations. It does not provide test results, analysis, or other analytical or assessment information.
Test incident report (TIR)	AR 73–1	Test organization or PM	A TIR contains test incident and corrective action data on test incidents as they occur. The tester is responsible for preparing test incident data for all tests identified in the TEMP. The PM is responsible for preparing corrective action data for all critical and major TIRs, as a minimum. See appendix V for information and format.
Test report	AR 73–1	Test organization	The test report is a formal document of record that reports the test results from conduct of a DT or OT test event. The developmental test report addresses the data and information obtained from DT and describes the conditions that actually prevailed during test execution and data collection. The developmental test report also includes an audit trail of any deviations from the planned testing. The operational test report includes findings-of-fact, based on the data collected.

Table U–1
Test and evaluation documents—Continued

Threat test support package (threat TSP)	AR 381–11	Materiel developer for DT; TRADOC (combat developer) for OT	The threat TSP is a document or set of documents that provides a description of the threat that the new system will be tested against. A threat TSP is required for all materiel systems when an operationally realistic threat is required. It identifies the threat requirements for the specific test, describes the threat to be portrayed and describes how the threat fits into the overall test execution and evaluation requirements. See paragraph 6–60 and appendix Y, threat testing, for additional information.
Training test support package (training TSP)	AR 350–1	TRADOC (combat trainer)	The training TSP consists of materials used by the TNGDEV or trainer to train test players and by the system evaluator in evaluating training for the new system. This includes training of doctrine and tactics for the system and maintenance on the system. The training TSP focuses on the performance of specific individual and collective tasks during OT of a new system. Prepared by the proponent TNGDEV and trainer, the training TSP represents the individual, collective, and unit training for the system when initially fielded. See paragraph 6–61 and AR 350–1 for additional information.
Transportability report	AR 70–47	Materiel developer	The Transportability Report is prepared for related systems with stated transportability requirements and is submitted to the MTMC Engineering Agency for approval. All information is provided for a comprehensive transportability engineering analysis. The report identifies transportability characteristics of newly designed, modified, or off-the-shelf procured materiel or components thereof. See AR 70–47 for report format.

Appendix V

Test Incident and Corrective Action Reporting

Section I

DA Form 7492, Test Incident Report

V–1. Purpose

The purpose of this appendix is to provide information on the processes and procedures for reporting DT and OT test incidents and corrective action information to the ATIRS that supports the CE process.

V–2. Overview

a. In order for the CE process to function effectively, program managers, CBTDEVs, FPs, system evaluators, and others participating in the acquisition process must be informed of system performance during tests in a timely manner in order to initiate corrective actions to system problems. The RAM IPT, RAM Scoring Conference, and Assessment Conference members use TIRs and corrective action information to form the basis for the assessment of RAM and ILS. (See AR 700–127.)

b. A sample DA Form 7492 (Test Incident Report) is depicted at figure V–1. A TIR is used to capture the minimum essential data on test incidents as they occur. It contains test incident data and corrective action (CA) data (see sec II) that are merged together by ATIRS at Aberdeen Proving Ground, MD. TIR preparation instructions are at section III of this appendix. Figure V–2 illustrates an example of special requirement data.

c. ATIRS is a restricted database that stores all test incident and corrective action information. It provides an Army standard method of electronically exchanging, storing, processing, and reporting on results of testing and other test-related information (such as non-RAM data on performance, firing records, required documents (for example, TEMP and ORD), and armor vulnerability). As such, ATIRS provides a centrally accessible T&E enterprise for programs and IPTs to facilitate quality assurance, evaluations, and modeling/simulation truth data.

d. ATIRS has three on-line interface modes—

(1) Terminal Mode. Through supplied menus, the user selects the data required, and it is displayed on the user's terminal screen in one of several fixed TIR formats. To use terminal mode, the user requires a personal computer running terminal emulation software.

(2) HP Information Access Mode. This requires the use of HP Information Access for Windows software, which permits easy, structured queries of the database. Information Access enables the user to perform data reduction, customize formats, and convert selected data to a variety of familiar personal computer formats, such as Lotus and Excel.

(3) Web Browser or Internet Mode (Vision). Under the ATC Vision concept, users are able to gain password-protected access to ATIRS via the Vision Web page located at (https://vision.atc.army.mil). Here, all TIRs are hyperlinked to flat text files, with further hyperlinks to digital galleries of photos, drawings, or other multimedia products.

e. The ATC, part of the DTC, administers the ATIRS. Assistance is available by electronic mail (atirs@atc.army.mil) or by submitting a request to Commander, U.S. Army Aberdeen Test Center, ATTN: CSTE–DTC–AT–TC–C (ATIRS Administrator), 400 Colleran Road, Aberdeen Proving Ground, MD 21005–5059.

V–3. Guidance and responsibilities

a. The tester (Government or contractor) is responsible for preparing test incident data for pre-FRP tests and those tests in the production and deployment phase that support a materiel release decision. Regulatory guidance requires the preparation of TIRs for all tests identified in the TEMP. Test incident data may also be prepared for other tests, as required by the program manager or other test sponsors.

b. The PM is responsible for preparing CA data for input into ATIRS for critical and major TIRs as a minimum (see para V–4*e* for definitions). While minor TIRs may not require corrective action, they should be reviewed to determine if there may be a requirement for any corrective action.

c. A CART (that is, comprised of the PM (chair), CBTDEV or FP, and the system evaluator) reviews all CA data and associated test incident data to verify that proposed corrective actions are appropriate and effective. The testers serve as advisors to the review team.

d. Malfunctions of standard ammunition or standard items used with developmental or experimental ammunition (for example, a charge used to propel experimental projectiles); issued for comparison purposes during research, development, or testing; used for seating, warming, spotting, or other purposes during testing; or being evaluated for lot acceptance purposes are excluded from the TIR submission requirement. For these instances, the reporting procedures outlined in AR 75–1 will be followed.

TEST INCIDENT REPORT (AR 73-1)	1. Release Date: 02 Jul 2001	
2. Test Title: PERFORMANCE OF Z SYSTEM	3. Test Project #: 1-ZZ-120-ZSY-012	4. TIR #: KX-D000021
5. Test Agency: MY PLACE 7. System: Z SYSTEM	6. Test Sponsor: PM Z SYSTEM 8. Original Release Date: 02 Jul 2001	

I - MAJOR ITEM DATA		
10. Model: MXYZ1 ZSYS CARGO	Test Life:	Units:
11. Serial #.: C-0217B-JB	21. 282.0	MILES
12. USA #: N1-1528	22. 23.1	ENGHRS
13: Mfr: ARMORED WHEELIES, INC.	23. 0.0	MHEHRS
14. Contract #: DAAE07-92-Z-X001	24. 0.0	MHECYC
15. Item #: 217	25.	

II - INCIDENT DATA	
30. Title: WIRE HANGING FROM WIDGET	40. Date & Time: 29 JUN 2001 1250 EST
31. Subsystem: WIDGET	41. FD/SC Step #: 05-
32. Incident Class: MAJOR	42. FS/SC Class: EFF
33. Observed During: OPERATIONS	43. Chargeability: HARDWARE/CFE
34. Action: MAINTAINED	44. Incident Status: PRELIMINARY
46. Categories: RAM	
47. Keywords:	

Test Environment:	Type:	Condition:
48. OPERATIONS	HILLY CROSS COUNTRY	DRY
49. Disposition: MISSING/LOST		

III - INCIDENT SUBJECT DATA		
50. Name: TERMINAL END	60. FGC: 06130112	
51. Serial #: NA	61. LSA #: NA	
52. FSN/NSN: UNKNOWN	Part Life:	Units
53. Mfr: UNKNOWN	62. 282.0	MILES
54. Mfr Part #: UNKNOWN	63. 23.1	ENGHRS
55. Drawing #: NOT SHOWN	64. 0.0	MHECYC
56. Quantity: 1	65. Next Assy: WIDGET	
57. Action: REPLACED	66. Serial #: NA	
58. (NOT USED)	67. Software Version #: NA	

IV - MAINTENANCE DATA			
70. Diagnostic Clockhours:	00:10	80. Type: UNSCHEDULED	
71. Diagnostic Manhours:	00:10	81. Level Used: UNIT	
72. Active Maint Clockhours:	00:02	82. Level Prsc: UNIT	
73. Active Maint Manhours:	00:02	83. Level Recm: UNIT	

V - INCIDENT/MAINTENANCE DESCRIPTION

90. Wire hanging from widget - system shutdown. Repaired.

At 1250, during operations, the system shut down. Organizational level maintenance was called. A wire with the terminal end missing was found hanging from the widget. Maintenance installed a terminal end and reattached the widget wire to the gadget screw. The system was restarted with no problem.

MAINTENANCE TIME BREAKDOWN

DateSt	DateEd	TmSt	TmEd	Level	Delay	Type	Dgchrs	Tmchrs	Dgmhrs	Tmmhrs	App
010630	010630	1310	1322	UNIT	NA	UNSC	00:10	00:02	00:10	00:02	Y

Figure V–1. Sample DA Form 7492 (Test Incident Report)

TIR Number: KX-D000021						Page Number: 2
PARTS DATA						
Nomenclature	FGC	MfrPart #	Miles	Level	Qty	Action
TERMINAL END	0613	UNKNOWN	282.0	UNIT	1	CONSUME

Name, Title & Phone of Preparer:	Releaser:
98. I. C. TEST TEST DIRECTOR DSN XXX-XXXX	99. I. RELEASE CHIEF, LIGHT TACTICAL VEHICLE BR DSN XXX-XXXX

VI - CORRECTIVE ACTION DATA

CA Status:	CA Entry Date:	CA Date Reviewed:
100. NOT REQD	101. 20 Jul 2001 REV # 0	102.
CA Date Proposed:	**CA Date Verified:**	**CA Date Completed:**
103. 20 Jul 2001	104.	105.

106. Developer's Analysis of Problem:
TERMINAL END WAS PULLED OFF - MAINTENANCE/FACTORY ERROR.

107. Status/Description of Corrective Action:
NO C/A REQUIRED

108. Test Results on Corrective Action:

109. Planned Production Implementation:

Figure V–1. Sample DA Form 7492 (Test Incident Report)—Continued

Example:

36. Special Requirements Data: Subsystem Code: B2 Hazard Severity: CRITICAL MRF: 020	 Para/Page: 21111/545 Sub Cause: GUN/TUR DRIVE & STAB Sub Cause Code: B2

Figure V–2. Sample block 36 special requirements data

e. Incidents from developmental software tests conducted specifically to surface software failures for correction by software programmers and engineers are reported in accordance with IEEE/EIA 12207.

V–4. Test incident data

a. The tester (Government or contractor) prepares the test incident data portion of the TIR (that is, header blocks 1–8 and sections I through V). Section IV to this appendix depicts the test incident data stream. Test incident data are prepared for each test incident occurring on an identifiable test item or system, regardless of the number of times the test incident occurs. Test incident data are also prepared for test incidents involving Government-owned products, such as items covered by a warranty or Government-furnished equipment. The MATDEV item manager will prepare a quality deficiency report (QDR) based on the TIR input (see AR 702–7 and AR 702–7–1). A separate QDR will not be prepared by the tester.

b. Some groupings of incidents are authorized for minor or extremely frequent occurrences that do not impact mission reliability. When an incident involves a problem that does not require maintenance (such as an inherent operational defect, safety, or HFE problem) and the problem can be determined by inspection or examination to be common to all samples of the test item that are accessible to the tester, the tester may prepare a single TIR that addresses the problem (in lieu of a TIR for each test item).

c. Test incident data will be prepared whenever the need arises during pretest, test, or post-test activities to report—

(1) The non-receipt of all or part of any applicable TSP, an inadequacy in the components of a support package (in particular the SSP), or an incomplete SSPCL.

(2) The start of test, to establish a record of the test start date, major component serial numbers (for example, engine or transmission), and the starting hours for the major components.

(3) The receipt of materiel in unsatisfactory condition for test.

(4) Any functional area characteristic, defect, or discrepancy (actual or incipient) that affects, may ultimately affect, or pertains to health, safety, environmental, operational suitability or effectiveness, or compliance with contract specifications or requirements documents of the test item/system (to include its hardware, operator or crew and maintenance personnel, prescribed training, publications, tools, diagnostic and support equipment, and associated software).

(5) The need for, or accomplishment of, a scheduled preventive maintenance check and service, if the maintenance data associated with the task are to be scored as chargeable and scheduled and will be used in the computation of maintainability statistics for the test.

(6) The need for, or the installation of, a modification to an end item or its associated software. Block 90 of the TIR will address the effects on previously reported test conditions.

(7) The need for installation, removal, adjustment, repair, or replacement of a component, assembly, or software for reasons other than above.

(8) The completion of off-item component or assembly repair (whether accomplished by the tester or by the contractor or manufacturer, on or off the test site) if such maintenance is not reported with the basic incident.

(9) The end of test, to establish a record of the test end date and the ending hours for the major components.

d. In addition, test incident data may report a summarization of subtest results (for example, performance, safety, or HFE) and/or the achievement of important milestones in the test program (for example, receipt or shipment of the test items, or commencement or completion of testing or a specific phase of testing).

e. Each TIR will be assigned a TIR classification value by the tester that reflects the degree of seriousness of the reported incident or test findings, regardless of cause, frequency, or expected probability of occurrence. The four acceptable TIR classification values are as follows:

(1) *Critical.* A critical TIR—

(a) Involves a catastrophic or critical hazard related to health or safety of personnel (death or severe injury or occupational illness; Categories I and II per MIL–STD–882).

(b) Involves a catastrophic safety hazard to the item/system under test (unplanned system loss; Category I per MIL–STD–882).

(c) Reports test results that make test suspension or termination advisable.

(2) *Major.* A major TIR—

(a) Involves a marginal hazard to health or safety of personnel (Category III per MIL–STD–882).

(b) Involves a critical safety hazard to the item/system under test (unplanned major system damage; Category II per MIL–STD–882).

(c) Reports the inability of the test item (including diagnostic equipment, tools, publications, software, and so forth) to meet a critical or essential functional area, design, or performance requirement.

(d) Reports subtest results that reflect inadequate performance.

(e) Involves two or more repetitive minor TIR incidents (see below) in which their cumulated effect could result in any of the above four conditions.

(3) *Minor.* A minor TIR—

(a) Reflects an actual or incipient malfunction, defect, hazard, or negative finding that does not qualify as critical or major.

(b) Reports subtest results that reflect marginal performance.

(4) *Information.* An Information TIR reports modification to the tested item, current condition of the tested item, test findings, subtest results, safety release information, or other types of information.

f. If the cumulative effect of two or more repetitive minor TIR incidents exhibiting the same manifestations meets the definition for a major TIR, then a major TIR may be written. This major TIR is written when the repetitiveness is considered serious enough to warrant a major TIR. As additional repetitive incidents occur, each incident is classified accordingly. This may result in additional major TIRs. Each such major TIR will describe how the repetitiveness justifies a major TIR and will list the preceding related TIRs that led to this major TIR.

g. A change or addition to information contained in distributed test incident data (that is, a more complete analysis, description of deferred maintenance, TIR reclassification, incorporation of scoring conference results, or addition of any other data that is required to complete or update the test incident data) will be accomplished by issuing revisions to the original test incident data. The revision will replace the original test incident data (or previous revisions) in ATIRS and in any other files (manual or otherwise) that may be created in ATIRS.

h. In revising previously submitted test incident data, the original data must be accounted for by reporting the information that has been revised in block 90 of the TIR. The basic TIR number assigned in block 4 is not to be altered; however, block 1 will identify the revision number and date. In those instances where the test incident data are revised to change the TIR incident classification, block 90 must provide rationale for the change.

i. The tester will electronically transmit the test incident data and revisions, if possible, by dial-in or TELNET (provided ATIRS access is authorized) or by electronic mail (atirs@atc.army.mil) to ATIRS using the data streams specified in figures V–3 and V–4. If a data stream is not possible, then the TIR form of figure V–1 (excluding sec VI) may be transmitted in ASCII format after coordination with the ATIRS administrator. No hardcopy test incident data will be submitted to ATIRS. Data will also be distributed to other users per agreements reached by T&E WIPT members.

j. If electronic transmission capability does not exist, then other electronic storage media of the test incident or corrective action information will be forwarded to ATIRS (address in para V–2*e*) for inclusion in the database. Media compatibility must be verified with the ATIRS administrator prior to mailing.

k. Distribution of test incident data that are prepared for tests other than those identified in the TEMP is limited to the addressees designated by the program manager, other test sponsor, or the tester.

l. The PM will prepare a listing, based on agreements reached by the T&E WIPT members, for distribution of photographs and classified test incident data. The VISION/ATIRS website (https://vision.atc.army.mil/) may be used to store pictures, graphics, video segments, and documents associated with the test incident for access by appropriate participants.

m. All test incident data must be validated before being released and distributed. The following timelines are provided as goals:

(1) *Critical test incident reports.* The tester notifies the program manager by telephone within 24 hours after detection of the incident and distributes the test incident data within 24 hours. Critical TIR data are transmitted electronically to the program manager, T&E manager, higher headquarters test manager, logistician, system evaluator, and the ATIRS administrator. Electronic message notification does not negate the requirement for accident reporting per AR 385–10.

(2) *Major, minor, and information test incident reports.* The tester prepares and distributes the test incident data as soon as the data have been validated. The goals are to distribute the test incident data within 3 workdays after detection of the incident or completion of the subtest for major TIRs, 5 workdays for minor TIRs and 10 workdays for information TIRs. Distribution should not exceed 10 workdays for any test incident data. Revisions to test incident data should be accomplished and distributed within 10 workdays after the need for the new information or correction is detected.

n. If test materiel is received in unsatisfactory condition for testing and it is the opinion of the tester that the unsatisfactory condition may jeopardize test objectives, invalidate test results, or render testing unsafe, the tester (after coordination with higher headquarters test manager) should notify the MATDEV by telephone.

(1) If corrections can readily be made with no delay in scheduled test initiation, the tester (after coordination with higher headquarters) should obtain telephonic concurrence from the program manager and initiate corrective actions or repairs. This means being able to place the item/system in serviceable condition in accordance with the contract specification or standards using available maintenance/repair capabilities. A major TIR will be written.

(2) If corrections cannot readily be made, the tester (after coordination with higher headquarters) should telephonically recommend test rescheduling, suspension, or termination and, if applicable, request disposition instructions for the test items or system from the MATDEV. A critical TIR will be prepared.

Section II

Corrective Action

V–5. Corrective action data

a. The PM prepares the CA data portion of the TIR form (see fig V–1, sec VI, and para V–12). Figure V–4 identifies the CA data stream. The information will reflect a program manager's analysis of the problem and the status or description of corrective action. If no corrective action is proposed, it will be documented in this section with appropriate justification. CA data will be prepared with the best information available at the time of preparation, even though the information may be incomplete.

b. Whenever possible, the PM should implement the necessary corrective actions during the conduct of the planned test program. This provides the system evaluator the opportunity to analyze the corrective action and determine the need for any additional testing. If a corrective action is implemented during testing, the tester will prepare test incident data on the incident.

c. Whenever narrative CA data items (blocks 106 through 109) are revised, the original data must be retained. Revisions may either add data or change erroneous information by citing the old and adding the correction.

d. Each corrective action taken is assigned a classification value that reflects the status of the corrective action. The acceptable corrective action status classifications are as follows:

(1) *Open.* An open corrective action status means that correction action has not been identified or proposed.

(2) *Proposed.* A proposed status means that corrective action is required and a potentially acceptable corrective action has been identified and proposed.

(3) *Verified.* This status means that corrective action is required and a corrective action has been verified as adequate by the test or analysis.

(4) *Reviewed.* The reviewed status means that corrective action is required and a CART has reviewed the proposed corrective action for appropriateness and effectiveness.

(5) *Completed.* This status means that corrective action is required and has been approved for production.

(6) *Incomplete.* An incomplete status means that correction action is required but could not be completed because of circumstances outside the control of the program (for example, no funds, program cancellation, court ruling, or manufacturer out of business).

(7) *Not required.* As implied, this classification means that a corrective action is not required.

e. The initial CA data will be submitted to the ATIRS administrator within 60 days of the date reflected in the TIR release date (block 1 of the TIR). Subsequent updates are submitted as appropriate.

f. A change or addition to corrective action information previously distributed is submitted to ATIRS as revised data. The revised data replace the original corrective action information in ATIRS.

g. The CA data will be electronically transmitted by dial-in or TELNET (provided ATIRS access is authorized) or by electronic mail (atirs@atc.army.mil) using the format of paragraph V–11. If the PM does not possess electronic distribution capability, the data will be prepared in accordance with the format of paragraph V–11 and provided on tape, floppy disk, or other electronic storage media to the ATIRS administrator (address in para V–2*e*) for input into the database. No hardcopies will be submitted.

h. The PM will prepare a listing of recipients (using the list agreed to by the T&E WIPT members) for distribution of basic CA data, photographs, classified information, or other information related to a corrective action. The VISION/ATIRS website (https://vision.atc.army.mil/) may be used to store unclassified pictures, graphics, video segments, and documents associated with the test incident or corrective action, for access by appropriate participants. Distribution of CA data for tests other than those identified by the T&E WIPT is limited to the addressees designated by the program manager.

V–6. Corrective action review team

a. The CART will review all CA data and associated test incident data and may meet separately or concurrently during any other convenient meeting where corrective actions might be discussed. Telephonic meetings are acceptable and encouraged. For corrective actions concerning critical and major TIRs involving a safety hazard, coordination must be accomplished with the safety community before the team convenes.

b. When any member nonconcurs with the proposed CA status decision, the PM (as chair) will attempt to resolve the issue. If it cannot be resolved, the PM will advise all members of the final decision. If nonconcurrence is still an issue, the member nonconcurring will raise the issue to the next level of management for resolution and concurrently advise the PM of action taken.

c. When the CA status is changed, the PM will transmit a CA data stream to ATIRS with the changed CA status information. CA status changes to "Reviewed" can occur only after—

(1) Appropriate concurrence by the CART.

(2) Withdrawal of nonconcurrence or resolution by immediate or final decision authority has occurred.

d. In support of the CE process, the PM will submit the changed CA status information to ATIRS as soon as possible or when the CART has reviewed and verified the corrective action.

V–7. Test and evaluation working-level integrated product team

a. The T&E WIPT plays an active role in developing the T&E program and integrating various disciplines and interest. Therefore, it is the perfect medium to effect necessary actions crucial to the TIR process. Prior to the first T&E WIPT (or any subsequent T&E WIPT, if required), the PM and tester will contact the ATIRS administrator for a list of possible values for the TIR blocks shown in paragraphs V–7*b* and V–7*c*. This list will form the basis for agreement or understanding of standard values at all meetings and ensure consistency of terms across all test phases and milestones.

b. At the first T&E WIPT, the PM and testers (or higher headquarters test representative) will lead discussion to establish acceptable unique values for block 2 (Test Title) and block 7 (System) so that consistency can be maintained between tests.

c. Prior to each test, the PM and testers (or higher headquarters test representative) will lead the following actions in subsequent T&E WIPTs to—

(1) Establish unique values to be registered with ATIRS for the following blocks:

(a) Test Agency (block 5).

(b) Test Sponsor (block 6).

(c) Model (block 10).

(d) Manufacturer (block 13).

(e) Contract No. (block 14).

(f) Subsystem (block 31).

(g) Failure Definition/Scoring Criteria Classification (block 42).

(h) Chargeability (block 43).

(2) Establish the format and units of measure to be registered with the ATIRS administrator for the following blocks:

(a) Test Life: Units (blocks 21–25).

(b) Part Life: Units (blocks 62–64).

(3) Discuss possible data values desired to be recorded during test for the following blocks:

(a) Action (blocks 34 and 57).

(b) Categories (block 46).

(c) Keywords (block 47).

(d) Test Environment; Type; Condition (block 48).

(e) Disposition (block 49).

(f) Type/Level Used/Level Prescribed/Level Recommended (blocks 80–83).

(4) Discuss security guidance and procedures on data handling. If competition sensitive data are involved, determine authorizations and data restrictions to ATIRS and submit to the ATIRS administrator.

(5) Establish a distribution list for the test incident and CA data to be used by TIR users (that is, PM, system evaluator, developmental and operational testers, logistician, CBTDEV or FP, and T&E manager). The list should include format (for example, data stream and TIR form text format), distribution method (for example, computer transfers, electronic mail, floppy disk, and hard copy), mail address, and electronic mailbox address for each recipient. For the electronic mailbox address, include the recipient name or point of contact and phone number.

(6) Determine recipients of hard copy information, such as classified photographs or other information related to test incident data.

(7) Determine data collection procedures for all of the test and commodity-unique additions.

(8) Determine capabilities and procedures of participants in implementing provisions of this handbook (for example, how contractor test incident data are processed for input to the system evaluator and the ATIRS administrator).

d. After the T&E WIPT and prior to commencement of testing, the program manager (in coordination with the tester) must then register the T&E WIPT acceptable values (see paras V–7*b* and V–7*c*) with the ATIRS administrator. Registration is accomplished through either electronic mail, facsimile, or in writing to the ATIRS administrator.

e. All additions to the blocks in the TIR or changes to the values agreed to by the T&E WIPT must be coordinated with the ATIRS administrator so that consistent, readily identifiable data can be stored, retrieved, and used.

V–8. Security

a. Because TIR data are transmitted, stored, and accessed via unsecured media, care must be taken to ensure that documents provided to ATIRS contain no classified information. In the event that information pertaining to a test incident is classified, the information will be published separately in a classified TIR and distributed to the listing agreed to by T&E WIPT members. In addition, an unclassified TIR referencing a classified TIR will be provided to ATIRS.

b. Instructions on handling classified documents from automated equipment are contained in AR 380–5. It is the responsibility of both originators and recipients to safeguard the classified information per AR 380–5. Since portion markings are not possible on the TIR, the individual blocks in a classified TIR need not be marked provided that—

(1) Classification markings are placed top and bottom.

(2) A statement is included in block 90 showing the source of the classification, full address of proponent, and declassification date/event/originating agency's determination required.

(3) A statement is provided in block 90 listing the classified block numbers and their classification levels. In addition, a statement will be provided to indicate that other blocks not listed are unclassified.

c. The tester should consult the program security classification guide for classification of program data or the program manager when classification of cumulated data is in question. The program manager should address operations security and competition sensitive implications of TIR information prior to commencement of pretest activities. If the reports are expected to contain operations security information, the program manager will notify the document originator and the ATIRS administrator of any limits to be placed on content, electronic mail distribution, storage, or interactive access per AR 530–1. Similar procedures will be followed for reports expected to contain proprietary or competition sensitive information.

d. Access to the ATIRS database is requested through the ATIRS administrator. As a default, Government users will have open access to ATIRS databases, unless the program manager or tester restricts the data access. All contractors are restricted and can access only data authorized by the program manager or tester. The T&E manager will have access to all data associated with their commodity command.

Section III

Test Incident Report Preparation Instructions

V–9. Introduction

This provides preparation instructions for the TIR form. Two data types are addressed—

a. Test incident data. Test incident data blocks are contained in sections I to V of the TIR form. Paragraph V–11 and figure V–3 provide instructions on preparing these blocks. The test incident data are the responsibility of the tester.

b. Corrective action data. CA data blocks are contained in section VI of the TIR form. Paragraph V–12 and figure V–4 provide instructions on preparing these blocks. The CA data are the responsibility of the program manager. These

data are provided to ATIRS using the data stream format specified in figures V–3 and V–4. ATIRS will reproduce the data into the TIR form format.

V–10. General instructions for completing a test incident report

a. Enter all data in either numbers, uppercase letters, or combinations thereof. The exceptions are section V (Incident/Maintenance Description) and blocks 106–109, which may be uppercase and lowercase letters.

b. Do not leave any blocks blank that are designated "must fill."

c. Left-justify all entries unless otherwise stated in the instructions.

d. When inputting data into ATIRS using the TIR form, follow exact placement and field lengths for the data elements to facilitate successful automated pickup of data.

e. When submitting electronically, submit all characters in ASCII format. The characters "|," and "\\" and the tilde are not permitted in the text as data values. Control and graphics characters are also not allowed.

f. If the TIR is distributed by hardcopy, use either 10-pitch or 12-pitch type. Do not mix pitch types; that is, data in 12-pitch should not be entered on a 10-pitch form.

V–11. Completion of sections I to V of a test incident report

Specific instructions follow for completing each area or section of the TIR. Additional items to note—

a. Sections III and IV. Sections III and/or IV can be omitted if the incident does not involve a part/component or maintenance action.

b. Required for reference. Some or all of the following materials for the item/system under test are required for reference while preparing TIRs:

(1) System support package component list (SSPCL).
(2) TMs/equipment publications.
(3) Maintenance allocation chart (MAC).
(4) Repair parts/special tools list (RPSTL).
(5) Logistic support analysis (LSA) control numbers from the logistics support analysis record (LSAR).
(6) Failure definition/scoring criteria (FD/SC).
(7) Technical Bulletin 750–93–1.

c. Test incident report header area. Fill in the TIR header area (blocks 1 through 7) on every TIR that is prepared.

(1) *BLOCK 1.* Release Date: (cols. 59–78, X(20) maximum). Enter the date (in DD MMM YYYY format) that the TIR was released for distribution. If a revised TIR is to be issued, change the release date to the release date of the revision, followed by a space, the phrase REV #, space, and the revision number. Allocate two spaces for the revision number. If only one space is used, fill in the first space with a 0. This is a must-fill block. Examples follow—

(a) Original TIR: 04 AUG 2001
(b) Revised TIR: 06 AUG 2001 REV # 01

(2) *BLOCK 2.* Test Title: (cols. 6–39, X(34) maximum). Enter the title that has been assigned to this test. This is a must-fill block. Contact ATIRS to specify the test title name prior to commencement of testing.

(3) *BLOCK 3.* Test Project #: cols. 45–64, X(21) maximum. Enter the test project number that has been assigned for this test. This is a must-fill block. For tests conducted by the DTC test centers, this will be the DTC Test Resource Management System number, complete with hyphens but without the test center funding code (for example, 1–VC–010–577–011). For tests conducted by activities outside of ATEC, other project numbers may be applicable. A project number is always required to maintain a unique record number for the project in the database.

(4) *BLOCK 4.* TIR #: (cols. 68–77, X(10) maximum). Enter the TIR number that has been assigned for this TIR. This is a must-fill block. Do not change the TIR number (because of TIR revisions, supplementation, or other reasons) once it has been assigned. The TIR number is made up of two parts as follows:

(a) The first part (first 4 characters) identifies the TIR as resulting from a specific test by a specific tester, keeping it apart from other tests by the same tester on a given system or model. The value assigned to this part is to remain constant for the duration of the test and will consist of the following:

1. The first and second positions are used to identify the tester. The value to be assigned will be the installation funding code for the tester (if Government) or for the program sponsor (if the test is being conducted by a contractor).
2. The third position is to contain a hyphen (-).
3. The fourth position is used for a test sequence code (values A through Z) that relate to the number of tests that have been performed by the tester on a given system or model (for example, assign "A" for the first test of a given system by a given tester). Zero-fill this position when not used.

(b) An example of the first part entry for the fifth test at the ATC on a given system is K2–E. After the alphabet has been exhausted (excluding "I" and "O"), use the first position from the second part of the TIR number for additional codes (for example, K2–AC). Zero-fill this position when not used.

(c) The second part of the TIR number is used for the unique portion of the number. Normally, the numbering should start with one and be indexed by one for each TIR; however, separate blocks of numbers may be reserved (for example, for major item types, individual end items, or subsystems) and applied sequentially when desired. Since this field will be sorted upon, do not allow any intermediate positions to be left blank. All numbers will be right justified and zero-filled (for example, K2–EA00001, KC–A000101).

(5) *BLOCK 5.* Test Agency: (cols. 19–38, X(20) maximum). Enter the name of the test agency (Government or contractor) that is responsible for the conduct and reporting of this test. This is a must-fill block. Contact ATIRS to specify the exact test agency name prior to commencement of testing.

(6) *BLOCK 6.* Test Sponsor: (cols. 59–78, X(20) maximum). Enter the name of the program sponsor for this test. This consists of both the sponsor name (or the sponsor acronym, if the name is lengthy) and office symbol. This is a must-fill block and should not be changed regardless of test phase. Contact ATIRS to specify the program sponsor name prior to commencement of testing.

(7) *BLOCK 7.* System: (cols. 14–27, X(14) maximum). Enter the name of the system, which encompasses all major items to be included in the test program. This is a must-fill block. Contact ATIRS to specify the system name prior to commencement of testing.

(8) *BLOCK 8.* Original Release Date: (cols. 68–78), X(11) maximum. Enter the date (in DD MMM YYYY format) for the test incident data original release.

(9) *BLOCK 9.* (Reserved).

d. Section I—Major Item Data. Complete this section for every TIR that is prepared. With the exception of block 10 and possibly blocks 13 and 14, specific entries in these blocks are applicable only if the TIR applies to a single sample of the major item under test (for example, an identifiable tank). If the TIR is to apply to more than one sample of the major item, enter an appropriate general response (for example, ALL, SEE BLOCK 90, OFF–ITEM, N/A) in each applicable space or leave them blank. If "SEE BLOCK 90" is used, enter the appropriate values in block 90, either in tabular or narrative form. Test planning personnel must establish acceptable test-unique values for blocks 10, 13, 14, and 15 and the units for blocks 21 through 25, as a minimum, prior to commencement of testing.

(1) *BLOCK 10.* Model: (cols 13–38, X(26) maximum). Enter the model, type, or series descriptor for the major item to which this TIR applies. This is a must-fill block. Contact ATIRS to specify the model name prior to commencement of testing.

(2) *BLOCK 11.* Serial #: (cols. 15–38, X(24) maximum). Enter the major item serial number, if applicable. If this TIR is used to document an off-item repair, enter "OFF–ITEM" in this space.

(3) *BLOCK 12.* USA #: (cols. 12–38, X(27) maximum). Enter the major item USA registration number (or tail number), if applicable.

(4) *BLOCK 13.* Mfr: (cols. 11–38, X(28) maximum). Enter the name of the manufacturer of the major item, if known. Contact ATIRS to specify the manufacturer name prior to commencement of testing.

(5) *BLOCK 14.* Contract #: (cols. 17–38, X(22) maximum). Enter the contract number, purchase order number, or document number that pertains to the obtainment of the major item, if known. Contact ATIRS to specify the contract number prior to commencement of testing.

(6) *BLOCK 15.* Item #: (cols. 13–38, X(26) maximum). Enter the code that has been assigned to the end item, group of test items, or type of data against which this TIR is being written. This block is to be used by the tester to assign test-unique codes to enable easier tracking of data. In general, test-planning personnel should establish acceptable test-unique item number codes prior to the start of test. Begin by determining whether all end items to be tested are to be of the same group within the system or of different groups. Then identify each end item to be tested in each group and assign a unique item number code for each end item. Also assign additional item number codes for any specific types of data that are to be recorded as pertaining to all items within a specific group (for example, PUBS for publication comments). When assigning these codes, consider how the test data is to be stored and retrieved. If data from one or more groups of end items are to be retrieved and/or consolidated, consider using the first characters of the code as part of the data retrieval selection criteria.

(7) *BLOCKS 16 to 20.* (Reserved) See paragraph V–14 (TIR Form Augmentation Procedures) of this appendix.

(8) *BLOCKS 21 to 25.* Test Life: (cols. 45–54, X(10) maximum) Units: (cols. 57–70, X(14) maximum). Enter the test life of the major item at the time of the incident and its corresponding units of measure. Up to five types of major item test life may be entered. Contact ATIRS to specify the test life format and units prior to commencement of testing. Examples of units of measure are miles, kilometers, rounds fired, flight hours, and so forth or abbreviations thereof. Test planning personnel should assign a specific unit of measure to each block for the duration of test, together with

required spacing, justification, and composition of the test life and unit of measure entries. If a life period other than test life is to be recorded, so indicate (for example, TOT ODOM MILES).

(9) *BLOCKS 26 to 29.* (Reserved) See paragraph V–14 (TIR Form Augmentation Procedures) of this appendix.

e. Section II—Incident Data. Complete this section for every TIR that is required. The blocks in this section pertain to summary information and basic incident data, to include the various classifications of the TIR and its scoring. Values entered in blocks 32 and 41 through 43 should be treated as preliminary when the TIR is first prepared. After the TIR has been scored at the RAM IPT or during the TIR closure process, submit a revised TIR (revising the values entered in blocks 32 and 41 through 43, as necessary) to reflect the various IPT agreements. The status of this scoring will be reflected in BLOCK 44. Test planning personnel will establish acceptable test-unique values for blocks 31, 34, 41, 42, 43, 46, 47 and possibly 48 and/or 49 prior to commencement of testing.

(1) *BLOCK 30.* Title: (cols. 13–38, X(26) maximum). Enter a title for the TIR or a brief summary of the information that is to be contained therein. This is a must-fill block. Be sure to stay within the space allowed.

(2) *BLOCK 31.* Subsystem: (cols, 17–38, X(22) maximum). Enter the name of the subsystem to which this TIR is to be charged to. This is a must-fill block. Contact ATIRS to specify the list of subsystem names prior to commencement of testing. The major item name and "none" are also acceptable values.

(3) *BLOCK 32.* Incident Class: (cols. 22–33, X(12) maximum). Enter the classification that is to be assigned to this TIR. This is a must-fill block. The only acceptable values are critical, major, minor, information.

(4) *BLOCK 33.* Observed During: (cols. 23–38, X(16) maximum). Enter the word or phrase that best describes the activity that was taking place when the event occurred that prompted the preparation of this TIR. Examples of typical test activity entries are INIT, Inspection, RAM–D, Safety Eval, Operation, Inspection, Non-Mission, Maintenance, Transport, Desk Audit, Log Eval, Perf Eval, and Env Eval.

(5) *BLOCK 34.* Action: (cols. 14–38, X(25) maximum). Enter the word or phrase that best describes any action that was taken or the major item following the event or incident. Prior to commencement of testing, contact ATIRS administrator to specify other acceptable values in addition to the examples below. Other values may be added by registering them with the ATIRS administrator. Examples of entries for actions taken on the major item are Cleared, Maintained, Suspended Test, Operated, Deferred Maintenance, None, or Open (maintenance has not been or was not completed).

(6) *BLOCK 35.* (Reserved) See paragraph V–14 (TIR Form Augmentation Procedures) of this appendix.

(7) *BLOCK 36.* May be used to enter subtest elements or as indicated in paragraph 6, TIR Form Augmentation Procedures, of these instructions.

(8) *BLOCKS 37 to 39.* (Reserved) See paragraph V–14 (TIR Form Augmentation Procedures) of this appendix.

(9) *BLOCK 40.* Date and Time: (cols. 58–77, X(20) maximum). Enter the date and time when the event occurred that prompted the preparation of this TIR. In the case of a TIR reporting a failure, malfunction, discrepancy, defect, maintenance task, or hazard, this will be the date and time that the problem or event occurred, began, or was detected. For other TIRs, this will be the date and time associated with determination of the need for the TIR, assuming that the requisite information is available. This is a must-fill block. Format for entry is day, space, month, space, year (DD MMM YYYY), space, 24-hour time (HHMM), space, and time standard (demilitarized zone), for example, 31 MAR 2001 2400 EST. Do not attempt to list a range of dates or multiple dates. Time and time standard may be omitted, if not known.

(10) *BLOCK 41.* FD/SC STEP #: (cols. 58–77, X(20) maximum). Enter the step number from the FD/SC decision tree flow chart for the test that best describes the rationale for the scoring of this TIR.

(11) *BLOCK 42.* FD/SC Class: (cols. 58–77, X(20) maximum). Enter the FD/SC classification that is to be assigned to this TIR. Contact ATIRS to specify the exact acceptable values prior to commencement of test. Examples of typical FD/SC classification entries are No Test, Non-RAM, SMA, MAF/MA, UMA, EMA/UMA, OMF/EMA/UMA, EFF, NEFF, SA/EFF.

(12) *BLOCK 43.* Chargeability: (cols. 60–77, X(18) maximum). Enter the FD/SC chargeability that is to be assigned to this TIR. Contact ATIRS for exact acceptable values prior to commencement of test. Examples of typical FS/SC chargeability entries are Hardware, Training, Environment, Software, Publications, Test, Conduct, Operator/Crew, Support Equip, GFE, Maint Personnel, Maint Hardware, or Not Applicable.

(13) *BLOCK 44.* Incident Status: (cols. 62–73, X(12) maximum). Enter the status that describes the method of arriving at values for blocks 32 and 41 through 43. Status entries are "Preliminary" or "Scored." If the tester scored the data, enter "Preliminary." Enter "Scored" if a formal committee such as a RAM IPT scored the data.

(14) *BLOCK 45.* (Reserved) See paragraph V–14 (TIR Form Augmentation Procedures) of this appendix.

(15) *BLOCK 46.* Categories: (cols. 18–31, 33–46, 48–61, 63–76, X(14) maximum). Enter the word or phrase from the following list that best describes the categories or test issues associated with this TIR. All applicable categories

will be submitted, with the primary category listed first. Acceptable values are Safety, O&O, Test Admin, Performance, Training, Software, RAM, Environmental, Log Support, Corrosion, Physical, Human Factors, and Design.

(16) *BLOCK 47.* Keywords: (cols. 18–31, 33–46, 48–61, 63–76, X(14) maximum). Enter the word or phrase of vital importance. All applicable keywords will be submitted, with the primary keyword listed first. Before using these keyword blocks, contact ATIRS for a list of presently used keywords prior to commencement of test. Other values may be added by registering them with the ATIRS administrator.

(17) *BLOCK 48.* Test Environment: (cols. 6–37, X(32) maximum). Describe the test environment that existed when the event occurred that prompted preparation of this TIR. Use this space for information in addition to that which was entered in block 33 (Observed During). When applicable, cite the appropriate paragraph of a military standard or specification in this space. For operational tests, this block normally contains the MP that the system was performing at the time the incident occurred. Contact ATIRS for other acceptable values in addition to those listed below prior to commencement of test. Other values may be added by registering them with the ATIRS administrator. Examples of test environment values are Automotive Performance, Armament Test, Electrical System Test, Logistics Test, High Temperature Chamber (Developmental Test), or Mission No. XXXXXXX (Operational Test).

(a) Type: cols. 39–60, X(22) maximum. Examples of environmental type values include Paved and Hilly Cross Country. Enter the environment type that best describes the type of environment in which the test is being conducted. Coordinate with ATIRS for a list of presently used phrases/words and to add any other phrases/words to the list prior to commencement of test. Vibration, Gravel, Swamp/Mud/Hog Wallow, Fuel Consumption, Washrack, Horizontal Slope, Obstacles, Belgian Block, Side Slope, Dynamometer, Fording Basins, Environmental, Chamber, Firing Range, Laboratory, Maint/Repair Shop, NA.

(b) Condition: (cols. 62–77, X(16) maximum). Enter the phrase that best describes the condition of the environment in which the test is being conducted. Coordinate with ATIRS for a list of presently used phrases/words and to add any other phrases/words to the list prior to commencement of test. Examples of typical environment condition values include Dry, Dusty, Heavy Mud, Ice And Snow, Ice, Snow, Light, Mud, Wet, Wet Snow, Ice and Fog, Sand, NA.

(18) *BLOCK 49.* Disposition: (cols. 19–77), X(16) maximum. Enter the word or phrase that best describes disposition of any defective (failed) materiel that pertains to this TIR. Prior to commencement of testing, contact ATIRS administrator for other acceptable values in addition to the examples below. Other values may be added by registering them with the ATIRS administrator. Examples of typical disposition values include Awaiting Instructions, Installed/Reinstalled, To Be Held Until (Date), Scrapped, Held for Failure Analysis, Reworked, Turned In To Supply, Cannibalized, Forwarded to Higher Level Maintenance, Missing/Lost, Returned to (Contractor Name), Other/See Block 90, Returned to (Sponsor Name), Not Applicable, and Shipped Per Sponsor.

f. Section III—Incident Subject Data. The blocks in this section provide for the description of the TIR subject part or assembly (if any) and its next higher assembly. Complete this section if the TIR pertains in any way to an identifiable part or assembly, a major subassembly or subsystem, the major item itself, or a component of its SSP. If the subject of the TIR is to be a group of parts or assemblies of a given type, make sure that all entries to be made in the various blocks apply to the entire quantity that is being described. If the parts or assemblies in the group have different values (for example, serial numbers, part numbers, part lives, and so forth), enter an appropriate general response (for example, SEE BLOCK 90, N/A, and so forth) in each applicable space or leave blank. Regardless of whether a part or a group of parts are of concern, provide in block 90 a tabulation of the parts used. Detailed instructions are provided in the block 90 instructions below. Because section III contains summaries of data, its blocks should not be used to count parts without close deliberations.

(1) *BLOCK 50.* Name: (cols. 12–38, X(27) maximum). Enter the name of the part or assembly being described as the TIR subject. Obtain it from the RPSTL. This is a must-fill block, if section III is used.

(2) *BLOCK 51.* Serial #: (cols. 15–38, X(24) maximum). Enter the serial number, lot number, or batch number for the item named in block 50.

(3) *BLOCK 52.* FSN/NSN: (cols. 15–38, X(24) maximum). Enter the Federal/National Stock Number for the item named in block 50. Obtain it from the RPSTL.

(4) *BLOCK 53.* Mfr: (cols 11–38, X(28) maximum). Enter the name of the manufacturer that built or produced the item named in block 50, if known or enter the Federal Supply Code of Manufacturer code from the RPSTL. Abbreviate as required.

(5) *BLOCK 54.* Mfr Part #: (cols. 16–38, X(23) maximum). Enter the manufacturer's part number for the item named in block 50. Obtain it from the RPSTL or from the part or assembly itself.

(6) *BLOCK 55.* Drawing #: (cols. 16–38, X(23) maximum). Enter the drawing number for the item named in block 50, if available. If desired, figure and item number references from the appropriate RPSTL may be entered in this block in lieu of a drawing number.

(7) *BLOCK 56.* Quantity: (cols. 16–25, X(10) maximum). Enter the quantity of the items that have been named in block 50. Refer to the introductory instructions for section III if the entry is to be greater than one. The number entered should be right justified. This is a must-fill block if section III is used.

(8) *BLOCK 57.* Action: (cols. 14–38, X(25) maximum). Enter the word or phrase that best describes what was done to the part or assembly named in block 50 following the event or incident. Enter NONE if no action was taken. This is a must-fill block if section III is used. Prior to commencement of testing, contact ATIRS administrator for other acceptable values in addition to the examples below. Other values may be added by registering them with the ATIRS administrator. Examples of entries for actions taken on a part or assembly are Inspected, Cleared, Tested, Diagnosed, Drained, Serviced, Operated, Flushed, Adjusted, Lubricated, Purged, Aligned/Repositioned, Disassembled/Assembled, Loaded, Calibrated, Removed, Added, Installed, Modified, Charged, Replaced, Torqued/Tightened, Slaved, Disconnected, Removed/Reinstalled, Unloaded, Repaired, Sampled Oil/Fluid, Cleaned/Washed, Overhauled, Repaired, Sampled Oil/Fluid, Cleaned/Washed, Overhauled, Safety Wired/Secured, Handled/Jacked, Rebuilt, Painted/Curing/Drying, and None.

(9) *BLOCK 58 to 59.* (Reserved) See paragraph V–14 (TIR Form Augmentation Procedures) of this appendix.

(10) *BLOCK 60.* FGC: (cols. 50–59, X(10) maximum). Enter the functional group code to which the item named in block 50 belongs. Obtain it from the RPSTL, MAC, or TB 750–93–1.

(11) *BLOCK 61.* LSA #: (cols. 51–77, X(27) maximum). Enter the LSA Control Number of the item named in block 50, if applicable. Obtain it from the LSAR for the system, if available.

(12) *BLOCKS 62 to 64.* Part Life: (cols. 45–54, X(10) maximum) Units: (cols. 57–70 X(14) maximum). Enter the true life, if known, of the item named in block 50 and its corresponding units of measure. If true life is unknown, enter test life. If the part or assembly is new, enter 0 (zero). Up to three (3) types of part life may be entered. An optional "When Repaired" of a maximum field length of 10 characters might be used on certain projects. In such case, only the first six characters of "Units" are printed on the TIR in order to fit required data on one line. Contact ATIRS for the part life format and units prior to commencement of testing. Test planning personnel should either assign a specific unit of measure to each block for the duration of test (the same as for blocks 21, 22, 23, 24, or 25) or designate one or more units of measure to be used with specific parts, assemblies, or subsystems of the major item (that is, the most appropriate units). Required spacing, justification, and composition of the part life and unit of measure entries should also be assigned. The program manager should provide part life data if the data are not known. Part life should be right justified. Decimal values and part life units should be left justified for blocks 62 through 64.

(13) *BLOCK 65.* Next Assy: (cols. 56–77, X(22) max). Enter the name of the next higher assembly to the item named in block 50. Obtain it from the RPSTL. The program manager should provide this information if the RPSTL does not exist.

(14) *BLOCK 66.* Serial #: (cols 54–77, X(24) max). Enter the serial number, if applicable, of the item named in block 65.

(15) *BLOCK 67.* Software Version #: (cols. 64–77, X(14) max). Enter the CSCI name when categories (block 46) or chargeability (block 43) is "Software."

(16) *BLOCKS 68 and 69.* (Reserved) See paragraph V–14 (TIR Form Augmentation Procedures) of this appendix.

g. Section IV—Maintenance Data. This section is used for summarizing data from all applicable maintenance tasks or actions that were performed on the end item identified in block 10 as a result of the event or incident being described on this TIR. Complete this section if maintenance was performed. If maintenance is known to be required but is not performed immediately, complete this section with all available known data, leaving the remaining spaces blank. When the maintenance is eventually performed, revise and update the data in this section and on the remainder of the TIR to reflect the additional information learned during the maintenance. Provide in block 90 a tabulation of the clockhours and manhours by maintenance level and type. Detailed instructions are provided in the block 90 instructions below. Because the blocks in section IV contain summaries of data, they will not be used to calculate supportability indices (for example, mean time to repair and maintenance ratio (MR)) without close deliberations. The tester establishes acceptable test-unique values for blocks 80 through 83 via the T&E WIPT process.

(1) *BLOCKS 70 and 71.* Diagnostic Clockhours/Manhours: (cols. 31–37, X(7) max). Enter the chargeable clockhours and chargeable manhours required to perform the diagnostic (fault location) portion of maintenance for all tasks or actions described on this TIR, regardless of maintenance level. Data are to be reported in the format HHHH:MM.

(2) *BLOCKS 72 and 73.* Total Maint Clockhours/Manhours: (cols. 31–37, X(7) max). Enter the chargeable clockhours and chargeable manhours required to perform all maintenance for all tasks or actions being described on this TIR, regardless of maintenance level. Include all diagnostic time from blocks 70 and 71. Data are to be reported in the format HHHH:MM.

(3) *BLOCKS 74 to 79.* (Reserved). See paragraph V–14 (TIR Form Augmentation Procedures) of this appendix.

(4) *BLOCK 80.* Type: (cols. 51–77, X(27) max). Enter the word or phrase that best describes the type of maintenance that was performed. Make sure that the entry does not conflict with any scoring entered in blocks 41 through 43. This is a must-fill block if section IV is used. Prior to commencement of testing, contact ATIRS administrator for other acceptable values in addition to the examples below. Other values may be added by registering them with the ATIRS administrator. Examples of entries for maintenance type are Unscheduled, Estimated, Scheduled, Simulated, and No Test.

(5) *BLOCK 81.* Level Used: (cols. 57–77, X(21) max). Enter the name of the highest maintenance level that was actually used to perform any of the maintenance being described in this TIR. This is a must-fill block if section IV is used.

(6) *BLOCK 82.* Level Prsc: (cols. 57–77, X(21) max). Enter the name of the highest maintenance echelon prescribed in the MAC that should have been used during this incident. Stated another way, this is the lowest maintenance level that is prescribed in the MAC or TMs as being authorized to perform all of the maintenance being described in this TIR. If no level is prescribed, enter "none" or "unknown," as applicable.

(7) *BLOCK 83.* Level Recm: (cols. 57–77, X(21) max). Enter the name of the maintenance level that the tester recommends for this maintenance, if different from the prescribed level entered in block 82. Prior to commencement of testing, contact ATIRS administrator for other acceptable values in addition to the examples below. Other values may be added by registering them with the ATIRS administrator.

(a) Examples of acceptable maintenance level entries in hierarchical order for blocks 81 to 83 are—

1. For Non-Aviation Systems: Crew/Operator, Unit, Unit/DS Assist, Contr Unit, DS/Unit Assist, Direct Support, Contr Direct Support, Contr Contact Team, General Support, Contr General Support, Special Repair Acty, Depot, and Contr/Unknown Level.

2. For Aviation Systems: Crew/Operator, Unit (AVUM), AVUM/AVIM Assist, Contr AVUM, AVIM/AVUM Assist, Intermediate (AVIM)/DS, Contr AVIM/DS, Contr Contact Team, Intermediate (AVIM)/GS, Contr AVIM/GS, Special Repair Acty, Depot, and Contr/Unknown Level.

(b) Values of "none" and "unknown" are also acceptable for block 82 but should not be used with blocks 81 or 83.

(8) *BLOCKS 84 to 89.* (Reserved) See paragraph V–14 (TIR Form Augmentation Procedures) of this appendix.

h. Section V—Incident/Maintenance Description. Complete this section for every TIR that is prepared. The use of uppercase and lowercase letters in block 90 is permitted and encouraged. Section V is a variable length narrative. If desired, it may be composed of several preprogrammed elements from other data entry systems (for example, short narrative, full description, and tabulated fillers and spaces for maintenance subtasks performed, parts used, and tools used).

(1) *BLOCK 90.* First Line: (cols. 6–77, X(72) max). Start the first line in column 6 on the same line as the number "90." On the remainder of the line, enter a brief summary of the incident that is being described on this TIR. For example, "Transmission clutch pack worn, no reverse, fault location only" or "Transmission removed and replaced because of worn clutch pack." Be sure to stay within the space allowed on the line. This is a must-fill line.

(2) *BLOCK 90.* Subsequent Lines: (cols. 2–77, X(76) max). On subsequent lines, fully describe the incident or event and any resultant maintenance tasks. This is a must-fill block. Use as many lines as are necessary and continuation sheets, if required. Use complete sentences and proper paragraph structuring, numbering, and indentation. Enter table headings and values as required to amplify the narrative. Use footnotes, if applicable. If desired, skip lines to separate paragraphs, space tables and table headings, and isolate footnotes.

(a) Provide answers to as many of these questions as possible: What happened? How did it happen? How was it discovered? Where did it happen? Under what conditions did it happen? Why did it happen? What actions, if any, were taken? Include additional description in instances where entries made in sections I through IV require further clarification. Include reasons or justification for incident classification assignments and scoring if they are not self-explanatory. For TIRs pertaining to an accident or environmental release, describe any resultant injuries or property damage. Include the word "safety" or "health" and a risk assessment code (for example, Cat I–A) per MIL–STD–882, if applicable.

(b) Whenever possible, indicate if the cause of the incident or event is improper design (for example, improper material, overstressing, interfering parts, or other design problems), improper manufacture, and operator/maintainer induced. Describe any positive actions or suggested solutions that appear capable of correcting the problem or would prevent future incidents of this type from occurring.

(c) TIRs, which report subtest results, will identify the name of the individual subtest and state the test results. Discuss the analytical procedures used and test measurement accuracy. Ensure that only factual data are contained in this paragraph. A caution "Preliminary Data -Subject to Further Review" leads into the following format of information: a. Reference Test Plan, subtest (fill in subtest), paragraph (fill in paragraph), dated (fill in date). b. Summary

of Results. c. Abbreviated Analysis. The program manager or evaluator may request additional data to be in the test incident data, if needed.

(d) Reference any hardcopy reports, sketches, photographs, or correspondence containing classified information on the incident or event that are being forwarded separately. Do not include any classified information in this block or, for that matter, in any other block on the TIR.

(e) Revise or update this description as more information becomes available or if additional maintenance tasks are performed as a result of the event or incident. Identify revised information with the heading on a separate line: "Revision," the date of the revision, and test life. Enter the name of the person who is responsible for the revised information, if other than shown in block 98. The test director is the person ultimately responsible for any TIR changes. For each TIR revision involving changes to data in sections I through IV, change the original data, then enter a brief description of the changes and the reasons for the changes. All original data in block 90 are retained during TIR revision to ensure data integrity. Revisions may add data or change erroneous data by citing the old and adding the correction.

1. *Maintenance time information.* After the descriptive narratives, provide a tabulation of maintenance time information for the maintenance actions performed as follows: maintenance level or echelon, maintenance type, clockhours, and manhours. After allowing for a blank line, begin the tabulation with the header "Maintenance Time Breakdown" starting in column 27. With no blank lines to separate, provide the maintenance information. Use the following header conventions in naming the columns (table V–1).

Table V–1
Header conventions for maintenance time

Content	Header	Maximum length	Beginning position
Date maintenance started (YYMMDD format)	DateSt	6	2
Date maintenance ended (YYMMDD format)	DateEd	6	9
Time started (4-digit 2400 hour clock format)	TmSt	4	16
Time ended (4-digit 2400 hour clock format)	TmEd	4	21
Maintenance level/echelon	Level	5	26
Administrative and logistic delay hours	Delay	10	32
Maintenance type	Type	4	43
Diagnostic clockhours (HHHH:MM format)	Dghrs	6	48
Total maintenance clockhours (HHHH:MM format)	Tmhrs	6	55
Diagnostic manhours (HHHH:MM format)	Dmmhrs	6	62
Total maintenance manhours (HHH:MM format)	Tmmhrs	6	69
Applicable (Y) or not applicable (N)	App	1	77

2. *Maintenance level content.* The maintenance level content is to contain no more than 5 characters. The maintenance type content is to contain no more than 4 characters. The characters allowed for these values are less than those allowed for blocks 80 and 81 because of the use of abbreviations to save space. The applicable time (App) is a marker that can be used to denote which maintenance periods are applicable for calculating supportability indices. Normally, "App" is not used. It is used as an aid to help differentiate maintenance times when not all times are usable for logistic supportability index calculations. The intent is to ensure all maintenance data are recorded. Use the following

abbreviations for the more common maintenance levels: CREW (Crew), UNIT (Unit), DS (Direct Support), GS (General Support), AVUM (Aviation Unit Maintenance), AVIM (Aviation Intermediate Maintenance), SRA (Special Repair Activity), DEPOT (Depot), CONTR (Contractor). Use the following abbreviations to indicate the more common maintenance types: NT (No Test), U (Unscheduled maintenance action), S (Scheduled maintenance action), EST (Estimated maintenance action), SIMU (Simulated maintenance action).

3. *Part information.* After the description narratives, provide a tabulation of parts used. After entering a blank line, begin the tabulation with the header "PARTS DATA" starting in column 35. Leaving no blank lines after the header, provide the following part information: nomenclature; FGC: numerical control identifications such as the serial number or FSN/NSN or manufacturer part number (whichever is available for the test item); part life; maintenance level/echelon prescribed for replacement; quantity; and action taken on the part. The program manager will provide the part information to the tester if information is lacking to complete the part information on a TIR. Use the following header conventions in naming the columns (table V–2).

Table V–2
Header conventions for part information

Content	Header	Maximum length	Beginning position
Nomenclature	Nomenclature	19	2
FGC	FGC	4	22
Serial number	Serial #	24	27
or FSN/NSN	FSN/NSN	24	27
or manufacturer number	MfrPart #	22	27
Part life	PartLife	7	52
Maintenance level/echelon	Level	5	61
Quantity	Qty	4	67
Action	Action	7	72

4. *Number of characters.* The number of characters allowed cannot exceed those specified for the corresponding blocks in section III and, depending on actual information content, can be even shorter. The nomenclature content is to contain no more than 27 characters (the same as block 50). The FGC code is only 4 characters long; the extra 10 character length is to accommodate extra information if needed. The units for the part life will normally be the same as used in block 62. In the header, the actual part life units will be substituted in place of "Part Life."

(3) *BLOCKS 91 through 95.* These blocks are to be used in a similar fashion as block 90. See paragraph V–14 (TIR Form Augmentation Procedures) of this appendix.

(4) *BLOCKS 96 and 97.* (Reserved to demarcate beginning of maintenance-time-breakdown and parts data in the data stream).

i. Test incident report responsibilities area. Fill in the responsibility blocks (blocks 98 and 99) on every TIR that is prepared. Each responsibility block may be three lines maximum, X(34) maximum per line. Leave one blank line between the command line and the names of the individuals. Test planning personnel should establish acceptable entries for some, if not all, of the information to be entered in blocks 98 and 99 prior to commencement of testing.

(1) *BLOCK 98.* Name, Title, & Phone of Preparer: (cols. 6–39, X(34) max). Enter the name, title, and telephone number of the person responsible for the content and validity of the information in this TIR. This is a must-fill block.

(2) *BLOCK 99.* Releaser: (cols. 45–78, X(34) max). Enter the releaser block as required by the tester. This is a must-fill block. This is the end of the test incident data portion of the TIR.

V–12. Completion of section VI of a test incident report

Specific instructions follow for completing blocks 100 through 109 of the TIR. Data stream examples are at figure V–4.

a. BLOCK 100. CA Status: (cols. 7–16, X(10) max). Enter Open, Proposed, Verified, Reviewed, Completed, Incomplete, or Not Reqd to indicate the status of the corrective action. This is a must-fill block.

b. BLOCK 101. CA Entry Date: (cols. 33–52, X(20) max). Enter the date (in DD MMM YYYY format) that the CA data are released for submittal. If the CA data are revised, the entry date changes with each new release and submission. A revision number is assigned for each revision. This is a must-fill block. Example follows—

(1) Original CA data: 04 OCT 2000
(2) Revised CA data: 06 OCT 1993 REV# 01

c. BLOCK 102. CA Date Reviewed: (cols. 59–69, X(11) max). Enter the date (in DD MMM YYYY format) that the CART reviewed the CA and verified it as appropriate and effective. Review may be by correspondence or electronic media (telephone, teleconference, email, facsimile). This date is entered when complete concurrence has been obtained (to include resolution of elevated issues). If review was by correspondence or electronic media, then use the date when final coordination was achieved. Block 100 would be annotated "Reviewed." This is a must-fill block if the CA review team verifies the CA.

d. BLOCK 103. CA Date Proposed: (cols. 7–17, X(11) max). Enter the date (in DD MMM YYYY format) that the program manager submits a potentially acceptable CA. Once entered, it will not change unless an error was made. Block 100 would be annotated PROPOSED. This is a must-fill block if a CA is proposed.

e. BLOCK 104. CA Date Verified: (cols. 33–43, X(11) max). Enter the date (in DD MMM YYYY format) that test or analysis verified the CA as adequate. Block 100 would be annotated "Verified." This is a must-fill lock when the CA action is verified as adequate.

f. BLOCK 105. CA Date Completed: (cols. 59–69, X(11) max). Enter the date (in DD MMM YYYY format) that the CA was approved for production and no further actions are required. This block is not a required entry for a CA status of Not Reqd. This is a must-fill block if block 100 contains "Completed."

g. BLOCKS 106 to 109. (cols. 2–77, X(76) max). Space is provided for entering four different types of narratives that pertain to the corrective action. The four narrative types, together with their respective block numbers, are as follows:

(1) 106. Developer's Analysis of Problem.
(2) 107. Status/Description of Corrective Action.
(3) 108. Test Results on Corrective Action.
(4) 109. Planned Production Implementation.

(5) Enter the block number and the title for the type of narrative that is being addressed; then prepare and enter the narrative. The use of uppercase and lowercase letters is permitted and encouraged. Use complete sentences and proper paragraph structuring, numbering, and indentation. Enter table headings and values as required to amplify the narrative. Use footnotes, if applicable. If desired, skip lines to separate paragraphs, space tables and table headings, and isolate footnotes.

(6) Use as many lines as are necessary for each narrative type. Complete one narrative and add a line of dashes before beginning another narrative. Complete the narrative before continuing on to another block. Keep the narratives in order by block number. Each of the narratives is a must-fill block.

(7) Limit the narratives to the corrective action and related incident reports. Reference any hardcopy reports, sketches, photographs, or correspondence containing classified information that is being distributed separately. Do not include any classified information in the narratives or, for that matter, in any other blocks.

(8) Revise or update the narratives as more information becomes available. Identify revised information with the heading on a separate line: "Revision" and the date of the revision. All original narrative data are retained during corrective action revision to ensure data integrity. Revisions may add data or change erroneous data by citing the old and adding the correction.

V–13. Pagination procedures

Page breaks are unnecessary in TIRs that are distributed electronically but may be present when hard copy distribution is being made. The location of the page break is left to the discretion of the preparer. Ideally, the page break should not leave a section title on one page and begin the data on the next. At the desired page break, end the page with the following centered line: "----------(continued on next page) ----------" Start each new page with a header of "TIR Number:" flush left and "Page Number:" flush right (see fig V–1 (page 2) for example). Regardless of the number of pages, always end the test incident data portion with the responsibility blocks (blocks 98 and 99) and a row of hyphens.

V–14. Test incident report form augmentation procedures

a. The TIR is a sequenced set of standardized record formats, each format containing either predetermined fillers or a combination of fillers and spaces for entering data. The form may be subjected to automated document processing. Successful processing by the method being used depends upon rigid adherence to the record sequence and the use and content of each record format.

b. During processing, the computer will look for particular data elements in specific locations on the form as depicted by the fillers. Therefore, fillers on the TIR form must not be altered with respect to location or content, and the locations and field lengths of the blocks for entering data should not be changed.

c. Limited provisions have been made to allow for tailoring of the TIR form by test planning personnel to accommodate test-unique or commodity-unique data entry blocks.

(1) Blocks 9, 16–20, 26–29, 35, 37–39, 45, 58–59, 68, 69, 74–79, 84–89, and 91–95 are reserved. These blocks will be used only after agreement from the T&E community. This decision will be made at an ATIRS Users Group Conference.

(2) In section II, block 36 may be used for added test-unique or commodity-unique data.

d. Special Requirements Data (block 36) consist of the following: name of the element, a colon, a space, and the element value. The element name, colon, space and element value are not to exceed 34 characters. Once a block is used, it will remain in use and maintained throughout the test. See figure V–2 for example.

e. Data collection procedures for all test-unique and commodity-unique additions should also be established and disseminated prior to start of test.

HEADER DATA

Field Name	Field Length (Fixed)	Field Position (Fixed)	Instructions
Data Item	1	1	0 – Indicates test incident information. Only the tester can originate this information. 1 – Indicates corrective action information. Only the test sponsor can originate this information. 2 – Indicates both test incident and corrective action information. Only the DTC Automated Data Collection System (ADACS) database can originate this combined information. 3 – Indicates ADACS data from ATTC.
Markings	1	2	0 – Unclassified 1 - FOUO
Version #	2	3-4	Version number; this version number is 0.
Sender's Phone #	20	5-24	Commercial Phone #.
Project #	20	103-122	Test Project # (TIRs only).
Submittal Date	6	123-128	Date of submittal in YYMMDD format.
Submitter	20	129-148	Point of contact responsible for submission of data.
Reserved	10	149-158	Reserved for future use.

TEST INCIDENT DATA

Block Number Block Name	Field Length (Maximum)	Instructions
~~1 Release Date	9	DD MMM YYYY
~~2 Test Title	34	
~~3 Test Project #	20	
~~4		

Figure V–3. Test incident data stream

TIR #/Revision	10/2	Omit slash if TIR is not revised
~~5		
Test Agency	20	
~~6		
Test Sponsor	20	
~~7		
System	14	
~~8		
Original Release Date	9	DD MMM YYYY
~~9		Reserved
~~10		
Model	26	
~~11		
Serial #	24	
~~12		
USA #	27	
~~13		
Mfr	28	
~~14		
Contract	22	
~~15		
Item #	10	
~~16		Reserved
~~17		Reserved
~~18		Reserved
~~19		Reserved
~~20		Reserved
~~21		
Test Life	10	
Life Units	14	
~22		
Test Life	10	
Life Units	14	
~~23		
Test Life	10	
Life Units	14	
~~24		
Test Life	10	
Life Units	14	
~~25		
Test Life	10	
Life Units	14	
~~26		Reserved
~~27		Reserved
~~28		Reserved
~~29		Reserved

Figure V–3. Test incident data stream—Continued

~~30		
Title	26	
~~31		
Subsystem	22	
~~32		
Incident Class	12	
~~33		
Observed During	16	
~~34		
Action	25	
~~35		Reserved
~~36		
Element Name:		Not to exceed 34 for name and value (including : and spacing)
Element Value:		
	Repeat for the number of names and values that are being collected.	
//	2	End of repeating blocks indicator.
~~37		Reserved
~~38		Reserved
~~39		Reserved
~~40		
Date Occurred	9	DD MMM YYYY
Time	4	
Time Standard	4	
~~41		
FD/SC Step #	20	
~~42		
FD/SC Class	20	
~~43		
Chargeability	18	
~~44		
Incident Status	12	
~~45		Reserved
~~46		
Category	14	May be repeated 4 times. Separate each item by a comma.
~~47		
Keywords	14	May be repeated 4 times. Separate each item by a comma.
~~48		
Test Environment	32	
Type	22	
Condition	16	
~~49		
Defective Material	59	

Figure V–3. Test incident data stream—Continued

~~50		
Name	27	
~~51		
Serial #	24	
~~52		
FSN/NSN	24	
~~53		
Mfr	28	
~~54		
Mfr Part #	22	
~~55		
Drawing #	23	
~~56		
Quantity	10	
~~57		
Action	25	
~~58		Reserved
~~59		Reserved
~~60		
FGC	10	
~~61		
LSA #	27	
~~62		
Part Life	10	
Part Units	14	If "When Repaired" is used, the displayed "Parts Units" length will be truncated to 6 characters.
When Repaired	10	
~~63		
Part Life	10	
Part Units	14	If "When Repaired" is used, the displayed "Parts Units" length will be truncated to 6 characters.
When Repaired	10	
~~64		
Part Life	10	
Part Units	14	If "When Repaired" is used, the displayed "Parts Units" length will be truncated to 6 characters.
When Repaired	10	
~~65		
Next Assembly	22	
~~66		
Serial #	24	
~~67		
Software Version	14	
~~68		Reserved
~~69		Reserved
~~70		
Diag Clockhours	7	hhhh:mm

Figure V–3. Test incident data stream—Continued

~~71		
Diag Manhours	7	hhhh:mm
~~72		
Total Maint Clockhours	7	hhhh:mm
~~73		
Total Maint Manhours	7	hhhh:mm
~~74		Reserved
~~75		Reserved
~~76		Reserved
~~77		Reserved
~~78		Reserved
~~79		Reserved
~~80		
Type	27	
~~81		
Level Used	21	
~~82		
Level Prescribed	21	
~~83		
Level Recommended	21	
~~84		Reserved
~~85		Reserved
~~86		Reserved
~~87		Reserved
~~88		Reserved
~~89		Reserved
~~90		
Incident Description	76	This is a repeating field. There is no need to repeat Block #.
//	2	Forward slash to end description for block 90.
~~91		Reserved
~~92		Reserved
~~93		Reserved
~~94		Reserved
~~95		Reserved
~~96		Additional Data – These are data blocks not covered anywhere above. Repeat as many as needed, including block #. If any data is missing, represent with a blank line.
Maintenance Start Date	6	YYMMDD
Maintenance End Date	6	YYMMDD

Figure V–3. Test incident data stream—Continued

Time Started	4	24-hour clock time
Time Ended	4	24-hour clock time
Maintenance Level/Echelon	21	Although a maximum of 21 characters is shown (following block 81 field length), only the first 5 characters are displayed on the TIR form in order to accommodate all specified Maintenance Time breakdown information on one line. Provide as much complete information as possible within the first 5 characters.
Admin & Logistic Delay Time	6	
Maintenance Type	4	
Diagnostic Clockhours	7	Although a maximum of 7 characters is shown (following blocks 70-73 field lengths), only the first 6 characters are displayed on the TIR form to allow all specified Maintenance Time Breakdown information on one line. Provide a much complete information as possible within the first 6 characters.
Total Maintenance Clockhours	7	
Diagnostic Manhours	7	
Total Maintenance Manhours	7	
Maintenance Chargeability	1	Yes (Y) or No (N) Repeat as many as needed, including block #. If any data is missing, represent with blank lines.
~~97 Nomenclature	27	Although a maximum of 27 characters is shown (following block 50 field length), only the first 19 characters are displayed on the TIR form to allow all specified Parts Data information on one line. Provide as much complete information as possible within the first 19 characters.
FGC	10	Although a maximum of 10 characters is shown (following block 60 field length), only the first 4 characters are displayed on the TIR form to allow all specified Parts Data information on one line. Provide as much complete information as possible within the first 4 characters.
Serial #	24	
FSN/NSN	24	
Manufacturer's Part #	22	
Part Life	10	Although a maximum of 10 characters is shown (following blocks 62-64 field lengths), only the first

Figure V–3. Test incident data stream—Continued

		7 characters are displayed on the TIR form in order to accommodate all specified Parts Data information on one line. Provide as much complete information as possible within the first 7 characters.
Part Units	14	Although a maximum of 14 characters is shown (following blocks 62-64 field lengths), only the first 7 characters are displayed on the TUR form in order to accommodate all specified Parts Data on one line. Provide as much complete information as possible within the first 7 characters. The information contained in this data element is displayed in place of "Part Life" in the header.
Maintenance Level/Echelon	21	Although a maximum of 21 characters is shown (following blocks 82-83 field lengths), only the first 5 characters are displayed on the TIR form in order to accommodate all specified Parts Data on one line. Provide as much complete information as possible within the first 5 characters.
Quantity	10	Although a maximum of 10 characters is shown (following block 56 field length), only the first 4 characters are displayed on the TIR form in order to accommodate Parts Data on one line. Provide as much complete information as possible within the first 4 characters. This entry must be numeric.
Action	25	Although a maximum of 25 characters is shown (following block 57 field length), only the first 7 characters are displayed on the TIR form in order to accommodate all specified Parts Data on one line. Provide as much complete information as possible within the first 7 characters.
~~98		
Preparer's Name	34	
Preparer's Title	34	
Preparer's Phone #	34	
~~99		
Releaser's Name	34	
Releaser's Title	34	
Releaser's Phone #	34	
-9		End of file indicator.

Example - Test Incident Data Stream

00 04105559413 jdoe@testplace. army.mil etc., etc., <cr> <lf>
~~1 <cr> <lf>

Figure V–3. Test incident data stream—Continued

92013 <cr> <lf>
~~2 <cr> <lf>
PQT OF SMALL WIDGETS <cr> <lf>
~~3 <cr> <lf>
9-ZZ-999-999-999 <cr> <lf>
~~4 <cr> <lf>
K2-B999999 <cr> <lf>
~~36 <cr> <lf>
Subsystem Code: <cr> <lf>
1 <cr> <lf>
Hazard Severity: <cr> <lf>
na <cr> <lf>
Sub Cause: <cr> <lf>
Main Battle Tank <cr> <lf>
Sub Cause Code: <cr> <lf>
1 <cr> <lf>
~~81 <cr> <lf>
ORG <cr> <lf>
~~82 <cr> <lf>
DS <cr> <lf>
~~83 <cr> <lf>
ORG <cr> <lf>
~~90 <cr> <lf>
Misalignment problem discovered. <cr> <lf>
During the initial phase inspection, an alignment problem was <cr> <lf>
noted between widge A and tab B. No further action was <cr> <lf>
taken at this time. <cr> <lf>
// <cr> <lf>
-9 <cr> <lf>

Figure V–3. Test incident data stream—Continued

HEADER DATA

Field Name	Field Length (Fixed)	Field Position (Fixed)	Instructions
Data Item	1	1	0 - Indicates test incident information. Only the tester can originate this information. 1 - Indicates corrective action information. Only the test sponsor can originate this information. 2 - Indicates both test incident and corrective action information. Only the DTC ADACS database can originate this combined information. 3 - Indicates ADACS data from ATTC.
Markings	1	1	0 - Unclassified 1 - FOUO
Version #	2	3-4	Version number.
Sender's Phone #	20	5-24	Commercial Phone #
Sender's E-Mail	78	25-102	
Project #	20	103-122	Test Project # (TIRS only)
Submittal Date	6	123-128	Date of submittal in YYMMDD format.
Submitter	20	129-148	Point of contact that submitted the data.
Reserved	10	149-158	Reserved for future use.

CORRECTIVE ACTION DATA

Block Number Block Name	Field Length (Maximum)	Instructions
~~0 CA Action #/Revision	10/2	This data field is not on the TIR form. It is used to distinguish one corrective action from another when multiple corrective actions occur on test incidents. Any convenient sequencing scheme may be used. If omitted, Corrective Action # will be generated. Do not use TIR # as Corrective Action #. When

Figure V–4. Test incident report corrective action data stream

		doing a revision, CA # and the revision # must be present. "Revision" is the revision number of the submitted DA data and is displayed in the CA entry data block.
~~3		
Test Project #	20	
~~4		
TIR #	10	This is a repeating field.
//	2	End of TIR # indicator.
~~100		
CA Status	8	
~~101		
CA Entry Date	9	DD MMM YYYY
~~102		
CA Date Reviewed	9	DD MMM YYYY
~~103		
CA Date Proposed	9	DD MMM YYYY
~~104		
CA Date Verified	9	DD MMM YYYY
~~105		
CA Date Completed	9	DD MMM YYYY
~~120		
Developer's Analysis of Problem	76	This is a repeating field.
//	2	End of Description for Block 106.
~~121		
Status/Description of Corrective Action	76	This is a repeating field.
//	2	End of Description for Block 107
~~122		
Test Results on Corrective Action	76	This is a repeating field.
//	2	End of Description for Block 108.
~~123		
Planned Production Implementation	76	This is a repeating field.
//	2	End of Description for Block 109.
-9	2	End of record indicator.

NOTE: Do not leave any blank lines at the beginning or end of this file.

Example - Corrective Action Data Stream

10 041055594 1 3 sponsor@matplace. army.mil etc., etc., <cr> <lr>

Figure V–4. Test incident report corrective action data stream—Continued

Appendix W

Survivability Testing

W–1. Overview of survivability testing

a. This appendix provides guidance on planning, executing, and reporting survivability testing to include E3, NBCCS, and Soldier survivability testing. This information differs from the live fire survivability testing discussed in appendix S in that it discusses survivability concerns related to the electromagnetic, nuclear, and Soldier environments. Survivability analysis and testing are included throughout the system design and verification process and conducted at the material, piece part, component, equipment, subsystem, system, and platform levels.

b. Survivability testing is a unique form of testing conducted primarily during DT, however, elements such as EW may be included in the OT. The scope of testing is driven by applicable regulations and may be tailored based on the customer requirements. The primary customer for survivability testing is the Army PM working in coordination with the T&E WIPT and system evaluator. Other customers may include other Army elements, joint Services, and private industry.

c. The testing discussions in this section build on the evaluation discussion provided in chapter 5 and appendix I, how testing is conducted and considerations in conducting various forms of survivability testing.

W–2. Survivability testing definitions

a. E3 refers to the impact of the electromagnetic environment upon the operational capability of military forces, equipment, systems, and platforms. It encompasses all electromagnetic disciplines, including EMC; electromagnetic EMI; EMV; EMP; hazards of electromagnetic radiation to personnel; ordnance, and volatile materials; and the effects of natural phenomena (lighting and static electricity). Generally accepted E3 requirements are discussed in MIL–STD–464.

b. The materiel survivability aspects are addressed through NBCCS. The characteristics that NBCCS testing must address are hardness, decontaminability, and compatibility. NBCCS is required for mission essential systems and equipment (see AR 70–75). DPG conducts biological, chemical, and contamination survivability testing and WSMR conducts nuclear (including thermal blast), HEMP, and nuclear radiation testing. Decontaminability and hardness require live agent testing in the DPG chemical surety labs. Compatibility requires human test participants (usually military personnel) to demonstrate use of the system while in MOPP IV in a simulated chemical attack environment.

c. Testing for Soldier survivability includes a range of analyses and test types, both survivability specific and not survivability specific, depending upon the type of system. When planning Soldier survivability testing, the potential effects of the system in its operating configuration and environment on Soldier survivability must be analyzed in order to determine those data required. For example, if a system has a potential reflective surface, such as a sight or other lens, the potential for increasing the visual signature of the Soldier and therefore their accessibility as a target must be determined. The goal is to provide data for proper system use and design to maintain or increase the ability of the Soldier to perform the mission while avoiding detection by the enemy. Light levels required to operate a system may require consideration and testing if the system mission involves blackout conditions. The effect of a system on the Soldier's ability to perform the mission without decreasing their ability to avoid detection by the enemy must be analyzed and appropriately tested.

W–3. Survivability test concerns

In planning the scope and type of survivability tests, the maturity of the system design and materials must be considered. Survivability requirements must be considered throughout system development; however, if the system is in breadboard or brassboard stages, it may be more appropriate to conduct analyses of survivability elements based on similar or past systems, vice actual hardware testing. If a system requires modifications in order to meet survivability requirements, these could involve both design and material changes. Therefore, as stated in AR 70–75 and the Defense Acquisition Guidebook, it is strongly desirable to begin the survivability assessment process early because deficiency corrections later in the system's acquisition process may involve costly decisions requiring system re-design.

W–4. Survivability testing platforms and interfaces

The operating environment and accurate physical identification of the configuration of the system under test must be considered in planning survivability testing, and must be replicated in testing to the fullest extent possible. In most system survivability tests, any platform mountings, interfaces, and connecting points must be tested along with the system under test itself. In some cases, the host platform (where applicable) will be included in the analyses and/or the tests. In some cases, a mockup or simulated host platform or interface can be included in the tests. The survivability

requirements of the host platform (where applicable) should be reviewed as part of test planning to maximize compatibility between those requirements and those of the system under test. Usually, the survivability requirements for the system under test should be no more stringent than those of the host platform system.

W–5. Destructive nature of survivability testing

The cost of the system under test, the number of test items available, and the destructive nature of many survivability tests must be considered in test planning. If items are costly and available systems few in number, then a series of survivability tests may be desired to be conducted using the same test items. Those survivability tests that are least destructive (such as EMI, EMC, and signature effects) should be conducted earliest, while the most destructive tests (that is, HEMP, lightning, and NBCCS) should be conducted last. The probability of a catastrophic or degrading effect of each test and the expected failure modes and robustness of the system under test itself should be considered, as should whether the system could be refurbished between tests.

W–6. Survivability testing of software systems

Both hardware and software must be included during survivability testing. A full-up system including mature software should be tested in most survivability tests so that the system can be operated after each test in order to determine any degradation.

W–7. Inclusion of a standard item in survivability testing

In cases when survivability requirements are stated relative to the current, standard, fielded system to be replaced, consideration must be given as to how that data will be obtained. If there are valid data on the current standard, fielded system, then those data can form the basis for comparison. If there are no such data, a standard item should be included in the applicable survivability tests for comparison to support analysis of the impact of any survivability failures. For example, if a test system is not survivable in one or more areas and the standard system is also not survivable, then the importance of that failure can be viewed with a different perspective than if a test system survivability were worse than the system it could replace.

W–8. Electromagnetic interference/electromagnetic compatibility survivability testing

EMI/EMC testing is conducted to ensure a system will operate within an intended environment or meet a system control specification. An electromagnetic system will both radiate and conduct emissions through antenna elements and connected cabling causing interference to neighboring and distant equipment. In this situation, a system operates as a source of EMI. A similar system may also be susceptible to radiated and conducted emissions either from neighboring or distant equipment. During this condition, the system or item is a victim of EMI.

a. Generally accepted requirements and procedures for testing are provided in MIL–STD–461. Test methods and requirements may be tailored to the procurement of the individual system or platform when analysis reveals that the requirements are not appropriate.

b. Although a system meets all specifications, it is ultimately important that the system be compatible with the neighboring fielded equipment that will be used in the operational environment. For example, if a motor is operated in close proximity to a radio, it is important to ensure this configuration is tested in various modes of operation. This is referred to as EMC testing. Often it may be difficult to determine the full extent of these various configurations, or large combinations of equipment may exist. When these conditions apply, the testers may consider selecting some worst case conditions based on an analysis of the situation.

c. EMI/EMC may also affect safety-critical functions such as firing circuits or operation of hazardous electromechanical equipment. EMI/EMC testing should be considered early in the development process since identified problems may require design changes impacting program cost and schedule.

W–9. Lightning effects survivability testing

The characteristics and causes of lightning and lightning effects are widely studied and will continue to be researched. Designers must be aware of the potential consequences of lightning effects and include appropriate measures for protection, such as grounded equipment and arrestors. The effects of lighting on Army equipment will range from no effect, mild disruption, to complete unrecoverable damage. Special consideration for lightning testing should be given to sensitive electronic systems, ordnance, and tall antenna/masts that will be deployed to areas with high occurrence of thunderstorms (that is, high keraunic number), high altitude above sea level, or systems that will be located in open terrain. Additional considerations may include electrical shock to personnel that may be required to operate equipment through an electrical storm. Lightning tests are conducted both for direct strike (that is, physical effects that often include burning, eroding, blasting, and structural deformation as well as the high pressure shock waves and magnetic

forces produced by the associated high current) and near strike lightning (that is, hazard resulting from electromagnetic fields). Generally accepted levels are defined in MIL–STD–464.

W–10. Electrostatic discharge control survivability testing

The system will be designed to control and dissipate the build-up of electrostatic charges caused by precipitation static (p-static) effects, fluid flow, air flow, launch vehicle charging, and other charge generating mechanisms to avoid fuel ignition and ordnance hazards, to protect personnel from shock hazards, and to prevent performance degradation or damage to electronics.

W–11. Electromagnetic pulse survivability testing

a. EMP is the electromagnetic radiation from a nuclear explosion caused by Compton-recoil electrons and photoelectrons from photons scattered in the materials of the nuclear device or in a surrounding medium. The resulting electric and magnetic fields may be coupled with electrical/electronic systems to produce damaging current and voltage surges. The EMP may also be cause by non-nuclear means. For more information, see AR 5–12.

b. During a high altitude nuclear detonation, gamma rays are released that set high energy electrons into motion. These electrons are subsequently deflected by the electromagnetic belt surrounding the earth and an EMP is created. This deflection can generate a voltage pulse of 50,000 V/m at a point 300 miles from the detonation, with a rise time of approximately 5,000 V/s. This is much more severe than a lightning strike, which has a field density of 3 V/m, 6 miles from point of discharge, and a rest time of 600 V/s. Because of the large magnitude of the voltage and frequency spectrum of an EMP, there are basically no "off-the-shelf" R–C or L–C filters that can effectively reduce or eliminate such an EMP.

c. Metal oxide semiconductor circuits and small area geometry semiconductors are especially vulnerable to the EMPs. Because of this vulnerability, effective suppression techniques and protective devices must be used to protect against EMP.

W–12. Electromagnetic vulnerability survivability testing

a. The characteristics of a system that cause it to suffer a definite degradation (that is, incapability to perform the designated mission) after being subjected to a certain level of effects in an unnatural (that is, manmade), hostile environment. EMV measures the system's incapacity to perform in the presence of hostile electronic attack. EMV is measured only in its own operational environment (either actual or simulated) and under conditions that take into account how susceptible the system is, how easily it can be intercepted by hostile intercept and direction-finding activities, the nature and extent of the hostile EW threat. For additional information, see AR 5–12.

b. The Battlefield Electromagnetic Environments Office as an element of DTC, develops, maintains, and operates the database for spectrum management, per AR 5–12.

W–13. Electromagnetic radiation hazard survivability testing

The hazards of electromagnetic radiation to fuels, electronic hardware, ordnance and personnel are normally segregated into three categories.

a. A system will comply with current national criteria for protection of personnel against the effects of electromagnetic radiation. Test, analysis, and inspections must verify compliance with established procedures and guidelines. Hazards of electromagnetic radiation to personnel relates to the fact that the body absorbs radiation, which can result in significant internal heating without the individual's knowledge. Such a situation may potentially result in a deleterious effects on an individual's metabolic process. Therefore, criteria have been established with the regards to acceptable limits. Hazards of electromagnetic radiation to personnel testing establishes the potential exposure levels emanating from a device or system.

b. Hazards of electromagnetic radiation to ordnance (HERO) relates to the susceptibility of ammunition and other explosive devices to electromagnetic fields emanating from other devices or systems. All explosive items that contain electrical initiating devices such as exploding foil initiators for example or similar items may initiate when exposed to high levels of electromagnetic radiation. Levels currently established are primarily based on possible shipboard transport or handling on ship and those levels found at U.S. military bases throughout the world. ATEC's DTC at WSMR and RTTC has the capability to conduct HERO on munitions although the Navy has the established capability for large-scale test items such as is conducted on armed helicopters. Lesser radiation levels, under those established for personnel safety, may be included during these tests to determine susceptibility of ammunition during preparation and uploading ammunition on an aircraft by personnel. Testing normally involves a requirement for specially configured items that provide a minimum hazard to personnel and equipment.

c. Fuels must not be inadvertently ignited by radiated electromagnetic energy. Hazards of electromagnetic radiation to fuel relates to the potential for fuels to initiate by radiated energy from onboard emitters and other external sources. Test, analysis, and inspections must verify compliance with established procedures and guidelines. RF energy can induce currents into any metal object, possibly resulting in a spark across a gap between conductors and resulting in ignition of fuel.

W–14. Information assurance survivability testing

IA is becoming an increasingly higher threat area and test scope and particulars will vary based on the system under test. Testing will be performed in order to evaluate this emerging threat. Testing will capitalize on the benefits and lessons learned from private and Government organizations to develop test methods and scenarios for identification of IA issues.

W–15. Nuclear weapons effects survivability testing

The nuclear effects occurring within the first 60 seconds of a nuclear detonation (INR), air blast, and thermal radiation, EMP are addressed under NWE. The nuclear effects occurring after 60 seconds of a nuclear detonation (neutron induced gamma radiation and fallout) are addressed as residual nuclear contamination under NBC effects. NBC survivability is approached in terms of mission effectiveness by establishing an NBC defensive architecture appropriate for the system. Personnel survivability aspects are addressed by employing NBC defensive equipment and TTP to ensure Soldier survivability. The material survivability aspects are addressed through NBC contamination survivability.

W–16. Electronic warfare survivability testing

WSMR performs directed energy laser vulnerability/susceptibility, high power microwave, and millimeter-wave testing using both contractor test requirement methodologies and classified criteria. The EPG provides various ground jammers for testing of tactical radios and navigation systems. The EPG also developed and utilizes in a limited manner along with the OTC simulated jammers. The applicability and use of simulated jamming should be considered to support testing when frequency clearance is a problem or frequency spectrum limitations prevail.

W–17. Signature effects survivability testing

Most requirements will pertain to the system under test being no more detectable or having no greater signature or footprint than the standard, fielded system. If valid data on a comparison system are not available, consideration should be given to including a comparison system in these tests. The operating environment of the system (for example, battlefield conditions, foliage, terrain, and mobility) should be considered in planning the test conditions. Footprints and detectability of a system will vary with its environment in the field (for example, stationary, moving, weather effects, light and atmospheric conditions); thus, a range of environment types and field conditions should be tested.

W–18. Directed energy survivability testing

Directed energy testing is an emerging area of concern with various requirements based on the system under test. Testing is conducted by WSMR, NM.

W–19. Nuclear, biological, and chemical contamination survivability testing

DPG, UT, conducts NBCCS testing, as described in AR 70–75. NBCCS testing must address the three elements of decontaminability, hardness, and compatibility. Decontaminability and hardness require live agent testing in the DPG chemical surety labs. Compatibility requires human test participants (usually military personnel) to demonstrate use of the system while in MOPP IV in a simulated chemical attack environment.

W–20. Functionality after survivability testing

Depending upon the system under test and its unique performance requirements and features, several measures may be required in order to determine the effects of survivability testing. In survivability test planning, the key performance indicators of the system should be identified and measured in a new system as a baseline. Then the series of survivability tests should be conducted, most likely on separate test items or in a series from least destructive to most destructive, each one followed by a visual inspection and by re-measuring of key performance indicators for that system. The purpose, mission parameters, operating procedures, and ILS concept of the system in the field must be considered when analyzing survivability results. For example, field procedures during decontamination may allow for some components or parts of the system to be removed and disposed of. If those components or parts were not NBC survivable, those results would not indicate that the entire system is not survivable. Another example is that some degradation in

certain functions may be allowable, and the system could still complete its primary mission, thus indicating adequate survivability.

W–21. Test sites and facilities for survivability testing

The following is a brief description of test sites and associated facilities available within the Army for conducting survivability testing discussed in this section.

a. WSMR, NM, is the largest overland missile range in the DoD and provides a great deal of capability in the survivability/vulnerability testing area. These test capabilities cover most requirements and, with a central location, have the benefit of greatly reducing logistics costs. The following major facilities are located at the WSMR.

(1) The Electromagnetic Radiation Effects Test Facility is the primary test facility for providing MIL–STD–464 environments and conducting EMC, both intra- and inter-system, and EMP (such as personnel, airborne, and p-static). The electromagnetic radiation effects facility coordinates and maintains multiple transmitters that are capable of producing approximately 200 V/m from 1 MHz through 48 GHz, three 70-ton turntables that are used to dynamically orient the system under test, and a large electromagnetic quiet room for making system emission measurements. The facility maintains all of the necessary instrumentation and support equipment required for this testing. WSMR also operates facilities for conducting EMP as well as a direct and near strike lightning facility for conducting tests in accordance with MIL–STD–2169.

(2) WSMR provides test capabilities for nuclear effects of electronics to include neutron, gamma total dose, gamma dose-rate, blast, and thermal effects. Along these lines, WSMR maintains an extensive electronic microcircuit nuclear response database of electronic component automated test and characterization capabilities in the Army, and support for electronic obsolescence and life cycle issues through the Radiation Tolerant Source of Supply Center. In addition, WSMR has been provides design consultation and guidance, and performing nuclear system modeling, simulation and predictions using electrical engineering techniques. The following combination of facilities (many conforming to ISO 9000) are capable of simulating the system's nuclear requirements as generated by the USANCA.

(a) Blast and thermal effects that may be experienced following a nuclear event can be simulated in the LBTS. The LBTS simulates the blast and thermal effects associated with a nuclear weapon detonation on an integrated nuclear battlefield and is capable of varying shock overpressures and duration independently. The world's largest airblast simulator is located at WSMR and can test systems as large as the UH–60 Blackhawk. It can simulate realistic blast waves from 10 to 10,000 kilotons and also peak static overpressures from 1 to 30 pounds per square inch (psi). The LBTS can also provide non-ideal airblast environments. The solar furnace facility provides thermal radiation testing of material. The solar furnace facility uses a very large mirror system to collect solar energy and then focus it through a computer-operated shutter onto the test object. Thermal simulations of environments between 10 and 1,000 kilotons can be provided.

(b) INR consists of the following:

1. *Neutron fluence effects.* The FBR produces neutron fluence test environments for semiconductor devices, electronic components circuit card assemblies, shop-repairable units, LRUs, subsystems and systems. The FBR is located inside a 15 meter (m) by 15 m by 6 m test cell that has a 4 m by 4 m entrance. Every Army system with a nuclear survivability requirement has been tested at the FBR as well as more than 6,000 different semiconductor devices.

2. *Gamma dose-rate effects.* The REBA and the LINAC provide environments for testing gamma dose-rate effects. The REBA is particularly suited for small systems or LRUs. The REBA provides a uniform test environment for threat level validation and engineering gamma dose rate testing. The LINAC is used for very small articles such as circuit boards. For large systems, gamma dose rate is performed at the High Energy Megavolt Electron Simulator (HERMES II), which is located 40 miles north of the WSMR main post area.

3. *Gamma total dose effects.* The gamma radiation facility (GRF) is the only DoD large gamma total dose test facility. Through the use of 1 to 13 large cobalt 60 sources, the GRF is capable of providing between 1000 rad (silicone) per second (rad (Si)/s) to less than 0.1 rad (Si)/s. Test items as large as tanks are tested in a test cell that is 6 m by 13 m by 5 m. Every Army system with a requirement has been tested at the GRF as well as more than 5,000 different semiconductor devices. The GRF can provide a vertical environment for testing of airborne radiacs and sensors. WSMR also operates the space radiation test facility for gamma dose and enhanced low dose rate sensitivity testing. The space radiation test facility provides unique testing of semiconductor devices and objects as large as 65 ft2 and is also certified under ISO 9002.

(c) Semiconductor Test Laboratory (STL) is used for electrical parametric and post-test evaluation of semiconductor devices and components. WSMR uses automated testers to evaluate radiation effects on semiconductor devices and components. The STL is connected by an air-vacuum transfer system to all radiation facilities for quick transfer to test devices/components. The STL provides ATEC's DTC and DoD a unique capability and has characterized more than 6,000 devices and components. Nuclear radiation survivability is achieved at the device/component/circuit level.

(3) WSMR uses three methods for EW/directed energy testing. The first is the Pulsed Laser Vulnerability Test Facility, which is the largest CO2 laser in the U.S. The second method is an arrangement WSMR has with the Air Force Research Laboratory at Kirtland Air Force Base, Albuquerque, NM. The Air Force Research Laboratory is the prime developer for high power microwave technology and the memorandum of agreement allows for the use of the latest technology on WSMR proper. The third is millimeter-wave testing at the electromagnetic radiation effects facility.

b. EPG, located at Fort Huachuca, AZ, is the Army developmental tester for C4I systems. The EPG facilities focus on supporting testing, modeling, stimulation and simulation for E3 requirements, with special emphasis on C4I. Key facilities include the following:

(1) The Blacktail Canyon EMI/TEMPEST Facility is equipped with indoor and outdoor facilities and equipment to conduct EMI and EMC testing in accordance with MIL–STD–464. EPG is also certified for conducting TEMPEST testing. Four indoor anechoic test chambers are available with a maximum size of 35 feet by 14 feet by 14 feet EPG also operates a Tem/Reverberation (TEM/REV) chamber that will fully immerse a system in a wide frequency range to quickly expose system problems.

(2) Tactical Radio and Force XXI Battle Command Brigade and Below (FBCB2) Test Bed facility was established to investigate EMI and EMC issues with tactical radio systems and their platforms. Testing conducted includes co-site EMI/EMC, and desensitization. The tactical radio test bed has the ability to setup a small to medium lay-down of emitters generating a ground truth RF environment for the item under test. The FBCB2 test bed may deploy over 100instrumented nodes throughout the Fort Huachuca reservation and surrounding areas representing slices of tactical units dispersed over realistic tactical operational distances.

(3) Electromagnetic Environmental Test Facility develops and deploys models, simulations, stimulation and data collection (hardware/software) to aid in E3 investigations and tests. Systems to conduct real-time monitoring and collection of data transmitted to/from equipment under test are continuously developed to meet changing customer requirements. EPG's "tester's toolbox" represents a totally unique Army asset supporting all phases of live, virtual, and constructive testing. Items of the toolkit include the Multi Functional Data Collector (MFDC), ORION, and the STARSHIP. The MFDC will collect and stimulate ground truth wide area network (WAN) and local area network (LAN) data of various formats. The ORION will assess a system's ability to operate in the intended E3 environment, including threat forces, and assess the influence of these environments. The STARSHIP is a test control center that provides command, control, and status display of various data collection hardware devices of the EPG, OTC, ATC, and Joint Global Positioning System Combat Effectiveness.

(4) The EPG currently uses a commercial network vulnerability scanner to provide automated, network-based security assessment and policy compliance evaluation for IA capabilities. The scanner performs both scheduled and event-driven probes of network communication services, operating systems, routers, email, Web servers, firewalls, and applications, to identify system weaknesses that could result in unauthorized network access. It generates reports ranging from executive-level trend analysis to detailed step-by-step instructions for eliminating security risks, including automatic links to vendor websites for software patches. The risk management approach measures the following three areas:

(a) Network architecture—including servers, firewalls, authentication controls, encryption engines, modem pools, remote access server (RAS) services, routers, printers, and connections to other organizations.

(b) Security policy enforcement—confirms proper configurations, ensures that users are not by-passing official policy and that all systems are reasonably secured against cyber attack.

(c) Security data correlation—comprehensively detects inter-related network-based vulnerabilities, learns from vulnerabilities detected in previous scans, and builds on this knowledge to discover additional vulnerabilities that would otherwise go undetected.

c. ATC, located at Aberdeen Proving Ground, MD, provides nuclear and electromagnetic survivability test facilities needed for general purpose and automotive systems testing.

(1) *Initial nuclear radiation.*

(a) Neutron effects. The APRF has a mobile, fast-burst reactor for testing of electronics against neutron effects. It is capable of producing self-limiting, high-yield, short-duration pulses or steady-state nuclear environments. Items can be located close to the reactor or outdoors at ranges of up to 2000 meters. For higher exposures, items of limited size may be located inside the reactor. The duty cycle of the pulse reactor for pulsing experiments is typically four to five pulses per 9-hour workday. Operating in the steady-state mode, the pulse reactor is capable of continuous operation up to 8 kilowatts and short ramp operations as high as 150 kilowatts.

(b) Gamma total-dose effects. APRF can supply gamma rays, which provide long-term effects and damage electronics through ionization. APRF can also provide a more realistic environment through use of the reactor to provide

gamma dose in combination with neutrons. APRF has two Cobalt 60 irradiators for producing 5,012 to 377,004 rad (silicone) per hour.

(c) Gamma dose-rate effects. In addition to damaging electronics through permanent ionization, gamma rays cause transient currents in electronic systems. The transients are proportional to the dose rate, and are usually expressed in rad (Si)/s. These transients may cause temporary damage (that is, latchup) or permanent damage (that is, burnout). APRF has a Physics International Model 538 FXR machine to simulate the prompt-gamma pulse of a nuclear weapon burst. Typical pulses are 87 nanoseconds (ns) full-width at half max (FWHM), with gamma dose rates of up to 4.6 by 1,011 rad (Si)/second or 1.0 by 1,012 rad (Si)/s in pinched beam mode at the faceplate and a rise time of approximately 30 ns. The FXR is movable along its track over a range time of 7 meters, and can be operated independently or adjacent the pulse reactor. In the latter position, the pulse reactor can be positioned in front of the FXR so that both machines can be operated in a combined sequence to simulate the complete INR environment. Typically, between four to six FXR pulses are possible per hour. Considerable flexibility exists in dose rates, pulse widths, and neutron fluence to simulate specific scenarios over practical exposure volumes. A combined environment allows a higher fidelity test than possible by exposing the system under test to the environments separately, since the nuclear threat is intrinsically a combined environment.

(2) *Electromagnetic Interference Test Facility.* ATC operates one of the largest double-walled shielded enclosures in the U.S. (94 ft by 60 ft by 16 ft enclosure with 16 ft by 16 ft access doors). This design provides a high degree of attenuation to magnetic (H–Field), electric (E-Field), and plan wave fields to assure excellent isolation from the outside electromagnetic environment. This isolation is required to successfully conduct EMI/EMC testing of electrical, electronic, and electromagnetic equipment. The size and structural integrity are features that allow the ATC to primarily conduct testing of large and heavy pieces of equipment and complete systems such as Army enclosures, tanks, generators, portable shielded enclosures, and component bench testing.

(3) *The U.S. Army Aberdeen Test Center Electromagnetic Interference Test Facility.* The ATC Electromagnetic Interference Test Facility utilizes a computer-controlled data acquisition system; presently covering the frequency range from 16 Hz to 40 GHz to measure and record radiated and conducted emission test data. The data can be provided in various forms to support customer requirements. Frequency synthesizers covering the frequency range from 16 Hz to 40 GHz are used to provide the signal to drive the power amplifiers used to conduct the electromagnetic susceptibility tests. The synthesizers can be operated manually or swept in continuous, step, or manual mode. A computer-controlled radiated and conducted susceptibility system is capable of providing signals having field intensity levels of 200 volts (V) per meter at frequencies up to 40 GHz. Spectrum analyzers are available to conduct spectrum analysis, ambient surveys, and frequency response tests of filters, and amplifiers. EMI-free metered electrical load banks are housed in the Electromagnetic Interference Test Facility to provide electrical loads for testing engine-driven power generators. One load bank can provide resistive or reactive loads adjustable from 0 to 200 kilowatts per kilovolt amperes (kW/kVa), 60 or 400 Hz, 120/208/220/480 V, single or three-phase, with adjustable power factors. A second load bank provides resistive loads adjustable from 0 to 2,000 amperes, at up to 30 V DC.

d. Infrared and RF survivability are usually lab bench tests that are nondestructive and require simulation of opposing force detection methods. Acoustic effects testing records the decibel levels of the operating system and compares this to human hearing capabilities over a range of distances. Subjective ratings and comments such as those obtained in human factors testing can also be used to indicate perceived acoustic signature. Acoustic signatures may require analysis with consideration to other acoustics in the operating environment. In visual signature testing, detection attempts must be made over a range of conditions and distances simulating field environments. Opposing force detection methods also must be simulated (for example, night vision goggles and thermal sights).

e. The RTTC, located near Huntsville, AL, at Redstone Arsenal facilities were developed for weapon systems and specialize in the test of missile systems. Indoor and outdoor facilities are capable of supporting small to large size test items. Test stands are available to ensure proper testing in the free field environment. RTTC can conduct automated EMC/EMI testing in accordance with MIL–STD–464. RTTC also has facilities for conducting direct-strike lightning tests. EW, electrostatic discharge, measurement and signature intelligence, and MIL–STD–2169 HEMP testing can also be conducted.

f. DPG West Desert Test Center is located in the Great Salt Lake Desert, approximately 75 miles southwest of Salt Lake City, UT, and is the Army developmental tester for chemical and biological defense equipment, smoke, and obscurants. The DPG facilities that support the NBCCS, Soldier survivability and obscurants/atmospherics testing include the following:

(1) *Combined Chemical Test Facility.* The Combined Chemical Test Facility consists of an administration area and laboratory facilities. The Combined Chemical Test Facility has 27 laboratories with 17 of the laboratories currently being certified for chemical agent use. The 17 laboratories have from one to four chemical fume hoods per laboratory. All laboratories allow testing to be performed at ambient temperature and humidity. Specially constructed

test fixtures can be placed in the fume hoods to conduct temperature and humidity-controlled testing. A fume hood is 5 ft wide, 5 ft high, and 3 ft long. When multiple hoods are in one laboratory, the hoods have pass through doors between the hoods. The hoods have controllers to maintain a 100 ft/min velocity.

(2) *Marvin Bushnell Materiel Test Facility.* The Marvin Bushnell Materiel Test Facility (MTF) is an environmentally controlled containment chamber for testing with chemical agents and simulants. MTF consists of three chambers, the multi-purpose test chamber, closed system chamber, and agent transfer chamber.

(a) The multi-purpose test chamber is a 50 ft long, 50 ft wide, and 30 ft high stainless steel chamber and is certified for use of live chemical agents. The chamber can also use chemical/biological vapors and aerosols for testing. It has a 16 ft wide by 24 ft high door, which can accommodate any military equipment that meets NATO shipping requirements, including fighter aircraft, helicopters, and ground vehicles. MTF is an air-tight chamber. The environmentally controlled glove box has a range from -40 °C to 60 °C with 5 percent to 95 percent relative humidity (RH). It can contain up to 1,000 mg/m3 concentration of agent and purge at 13,000 cubic feet per minute. The chamber has a 5-ton pneumatically driven bridge crane.

(b) The closed system chamber is 25 ft long, 250 ft wide, and 25 ft high stainless steel chamber. It has pneumatically sealed air locks and can purge at 5,300 cubic feet per minute. The environmentally controlled glove box ranges from -40 °C to 60 °C with 5 percent to 95 percent RH.

(c) The agent transfer chamber is 25 ft long, 25 ft wide, and 30 ft high. The chamber has two fume hoods, an agent storage vault and a glove box test area.

g. The superchamber is 16 ft by 25 ft by 10 ft high (only 8 ft of working space). The chamber is capable of testing from -10 °F to 130 °F. The chamber has a total of 16 glove ports along both sides. The superchamber is all stainless steel. One end of the chamber has a foldable worktable. The chamber will accommodate dissemination of chemical agents as vapor or aerosol droplets. The air inside of the chamber can be exhausted through a sacrificial filter system. The superchamber is actually located within a chamber that has its own engineering controls. Entrance can be accomplished through either end of the superchamber.

h. Recently remodeled using high-tech control systems, the defensive test chamber, a 30 ft by 50 ft by 30 ft high stainless steel chamber, is used for testing with simulants, and can replicate a variety of environmental conditions. Temperatures inside the defensive test chamber can range from -20 °F to 120 °F, with 0–95 percent RH. The chamber can be operated as a wind tunnel by increasing the wind speed, thereby providing a good mixture of simulant vapor clouds. Testers can maintain wind speed at 5.4 mph at 60 percent fan speed and 7.5 mph at 80 percent fan speed.

i. The Decontamination Pad consists of a concrete pad on a raised earthen mound. The pad has a raised rim around its perimeter and through the center of the pad. The pad is sloped to allow liquids to flow into sealed troughs for collection. The troughs have a pump for removal of liquids. There are lights surrounding the pad to allow testing at night. The pad also has a curtain system to minimize spray from escaping into the environment. The pad is split into two equal sides that are 40 ft by 60 ft. Vehicles can be driven onto each side of the pad but not from one side directly onto the other side.

j. The Lothan Solomon Life Sciences Test Facility (LSTF) is a 32,000 square foot facility that has Biosafety Level 2 and 3 (BL–2 and 3) laboratories and chambers enabling testing and aerosolization of simulated and actual agents of biological origin (ABO). State of the art infrastructure, chambers, and technical expertise of the Life Science Division provides a current and versatile facility for T&E of biological detection components and systems. The testing regime includes laboratory testing, simulated environmental aerosol challenges in test chambers and controlled outdoor aerosol challenges. Test items may be challenged with ABOs or simulants, in liquid or aerosol form, in indoor chambers. Tests are conducted only with simulants on the outdoor test grids. There are currently over twenty ABOs in use in the laboratory. Included is Yersinia pestis, Francisella tularensis, Coxiella burnetii, Bacillus anthracis, Venezuelan Equine Encephalitis virus, Botulinum toxin (BOT), Staphylococcal Enterotoxin B (SEB), and ricin. Laboratory, chamber, and field testing combine to provide baseline characteristics, operating parameters and detection thresholds for biological sampling and detection devices. The LSTF was designed with two environmentally controlled chambers for challenging the system under test with aerosolized biological test agents: the Aerosol Simulant Exposure Chamber (ASEC) and the Containment Aerosol Chamber.

(1) The ASEC is a 13 ft by 12 ft by 11.5 ft stainless steel chamber in which temperature, RH, and simulant concentration are controlled and maintained. Temperatures ranging from −5 °C to 40 °C and relative humidities ranging from ambient to 100 percent can be maintained. The ASEC has an air mixing and computer controlled dissemination system enabling the repetitive generation of consistent and homogenous simulant aerosol clouds. Battlefield interferents can be introduced into the ASEC to challenge the system under test, but at this time, there is no system to quantitatively control their dissemination or measure concentration.

(2) The Containment Aerosol Chamber is a 5 ft by 5 ft by 16 ft stainless steel containment chamber in which temperature, RH, and ABO concentration can be controlled and maintained. Temperatures ranging from −5 °C to

40 °C and RHs ranging from 0 percent to 100 percent can be maintained. The Containment Aerosol Chamber is equipped with air mixing and biological agent dissemination capabilities in addition to BL–3 containment. All incoming and exhaust air is HEPA filtered and work is performed utilizing glove ports and uniquely designed standup halfsuits. Interferents can be introduced and tested but control of concentration is limited.

(3) The environmental test chamber located in the LSTF is used for the biological simulant (Bacillus subtilis niger var. (BG) and nuclear fallout simulant (ZnS (FP))). The test chamber is 1.5 meter high by 1.5 meter wide by 1.5 meter long and is capable of controlling temperature (−20 °C to +100 °C) and humidity (0 to 100 percent).

k. Soldier survivability tests and facilities follow.

(1) *Man-in-simulant test.* The man-in-simulant test provides data to characterize and evaluate the chem-bio protective clothing and equipment system performance in vapor challenges for both local and systemic effects and identifies any conditions associated with increased vapor penetration. The man-in-simulant test is conducted in the Defensive Test Chamber. Two types of samplers are used during the system test. Passive sampling devices are placed in designated locations to measure the total amount of simulant that penetrates the protective system. Real-Time Samplers Miniature Infrared Analyzers provides a near real-time measurement of challenge concentrations.

(2) *Aerosol testing.* Provides data to characterize and evaluate the system performance of protective suits/equipment in aerosol challenges for both local and systemic effects; identify any conditions associated with increased aerosol penetration. A challenge aerosol (that is, simulant) concentration is generated using a flourescently tagged inert particles in a specially designed test chamber while wearers perform a fixed set of exercises. Upon exiting the chamber, the wearers are sampled using a liquid extraction from the skin, the extracted fluid is analyzed for the amount of simulant present. Wearers are also photographed under black light to identify the relative amounts of simulant present at each sampling site.

(3) *Smartman mask tester.* This fixture is used to test chemical protective masks by placing them on a zinc head form that has been constructed to simulate a Soldier's head and to allow installation of a protective mask. A breather pump is used to draw air into the head form, simulating human breathing. A peripheral seal, mounted in a channel on the head form, is inflated to compress against the inside of the mask, ensuring an optimal mask/fixture seal. This head form is mounted inside a temperature and humidity controlled chamber that is capable of containing chemical agent vapors and is challenged at specified liquid for vapor, or a combination of both, agent concentration. Sampling locations at the nose and eye allow the vapor concentration inside the mask to be monitored. Challenge concentration is measured by a near-real time instrument.

(4) *Protection factor test.* The protection factor test determines how well the protective mask fits the face of the individual, since completeness of the face seal is critical parameter for respiratory protection. The protection factor test examines the face seal leakage of the protective mask while each wearer performs 10 standard, 1-minute exercises surrounded by a corn oil, aerosol cloud in a chamber. The aerosol count within the mask is constantly monitored via sample tubes inserted through the mask's side voicemitter and drink tube monitoring eye and nasal cavities, respectively. The aerosol measurements are made using a forward light scattering laser photometer driven by a data acquisition system.

W–22. Obscurants survivability testing

DPG conducts testing to address the effects of obscurants and survivability of systems in obscurants. These are field tests that provide data to determine whether the system can operate and survive in an obscurant environment.

W–23. Survivability tester responsibilities

a. ATEC's DTC, as the survivability tester, will participate in the T&E WIPT and other working groups so as to provide expertise needed to develop a survivability test program to meet the needs of the system evaluator. When reviewing program documentation, the survivability tester will identify survivability test concerns to include, absence of testing in the TEMP, absence of testable requirements in the requirement documents and inadequate test procedures or facilities. ATEC's DTC will provide appropriate input to the TEMP needed to identify the survivability testing to be performed.

b. ATEC's DTC will coordinate with the MATDEV or PM to obtain detailed information on the system description needed to assess survivability and to implement a thorough and carefully conducted test. A cost estimate will be prepared for the customer and funding provided prior to start of testing. A test plan will be prepared and coordinated with the system evaluator and other members of the T&E WIPT as appropriate. Testing will be conducted in accordance with the test plan. TIRs will be provided to document incidents as they occur. Interim test results may be provided to the T&E WIPT as needed. A test report will be issued at the conclusion of the survivability test program to support the system evaluation and program decision process.

W–24. Summary

It is neither practical nor feasible to make every system/subsystem fully survivable on the battlefield. The program sponsors, in coordination with the system evaluator, developmental and operational testers, MATDEV, and CBTDEV must assess the risk associated with each of the survivability areas to determine whether the risk is acceptable. Safety of personnel and munitions is critical and protection is generally required to preclude unsafe situations. The most stringent intended environment will be used to identify system shortcomings.

Appendix X

Operational Testing Entrance Criteria Templates

Section I

Templates Uses

X–1. Overview

Proper risk management requires the development of a systematic, disciplined plan to identify problems and risks. A proven risk management technique is to examine the successes, failures, problems, and solutions of similar (or past) programs for "lessons learned" that can be applied to current programs. Another technique is to systematically comb through the entire set of programs using specific decision criteria based on historical data. The establishment of entrance criteria combines these techniques with a system for assigning responsibility and tracking accountability for results.

X–2. Scope

The matrix of templates in table X–1 cover a broad range of subjects that have historically impacted systems transitioning from DT to OT. Not all templates may apply to every program. The templates are arranged in three major groups: Test Planning and Documentation; System Design and Performance; and Test Assets and Support. These templates may be used in conjunction with the templates in DoDD 4245.7–M. All templates are designed to increase the visibility of potential risk factors and facilitate a streamlined, executive-level review. Reference the appropriate figure for additional template information.

Table X–1
Operational testing entrance criteria matrix of templates

Test planning and documentation		System design and performance		Test assets and support	
Schedule (see fig X–1)	Concept of operations (see fig X–6)	Contractor testing (see fig X–12)	Production rep articles (see fig X–17)	Test team training (see fig X–22)	Packaging, handling and transportation (see fig X–28)
Requirements (see fig X–2)	TEMP (see fig X–7)	Developmental testing (see fig X–13)	Interoperability and compatibility (see fig X–18)	Personnel (see fig X–23)	Support agreements or contractor support (see fig X–29)
AoA (see fig X–3)	OT Event Design Plan (see fig X–8)	Live fire testing (see fig X–14)	Software development (see fig X–19)	T&E infrastructure (see fig X–24)	Threat systems (see fig X–30)
STAR (see fig X–4)	Deficiency ID and correction process (see fig X–9)	System performance (see fig X–15)	Safety reviews and certifications (see fig X–20)	M&S (see fig X–25)	Technical data (see fig X–31)
Maintenance concept (see fig X–5)	Security planning (see fig X–10)	System maturity (see fig X–16)	Deficiency resolution (see fig X–21)	Support equipment (see fig X–26)	CTSF testing (see fig X–32)
	Configuration management plan (see fig X–11)			Sufficiency of spares (see fig X–27)	Joint interoperability testing (if required) (see fig X–33)

X–3. Team effort

Since any risk reduction process is a team function, PMs must provide the right organizational structure and continuous motivation to make it effective. Risk is eliminated only when existing conditions that cause problems are changed. These changes will typically occur at levels not normally visible to senior decision makers. This process should start at the earliest date possible but should then culminate by OTRR #1 (that is, 270 days prior to start of OT). The formal OTRR process (see para 6–45) will track any incomplete template.

X–4. Starting early
To be most effective, the development of OT entrance criteria must begin as early as practical after the initiation of a new program. Early on, the PM will use the templates grouped under Test Planning and Documentation (Templates 1–11). These templates look past the system itself to areas upstream in the acquisition process where earlier fixes to problems generate large future paybacks. The System Design and Performance (Templates 12–21) focus on activities after Milestone B and before OT begins. The Test Assets and Support (Templates 22–33) helps ensure all required assets come together in preparation for OT.

X–5. Series of operational test readiness reviews
Entrance criteria are considered in a series of OTRRs culminating in a determination of readiness for OT. The T&E WIPT should decide how to structure each entrance criteria template for the program. The T&E WIPT should decide on the best forum for conducting the reviews. Some suggestions are using the T&E WIPT or, if the acquisition program warrants, forming a special OTRR group.

X–6. Frequency of reviews
PM, in coordination with T&E WIPT, should establish the schedule required to complete the templates. In general, the frequency of reviews should increase as the program approaches OTRR #1. Early in the development program, a year between reviews may be sufficient, but as OTRR #1 draws near, reviews could be spaced at 3 to 6 week intervals. As reviews proceed, PMs may find some templates are chronologically too early (or too late) to have immediate impact on a program. All templates and line items should be covered at each review to ensure adequate lead times are planned, to address requirements changes, and to correct past oversights. See table 6–3, Recommended OTRR dates.

X–7. Review
A thorough review of all system requirements and resource needs is the first step in assessing a program's readiness to begin OT. Each participant (subject matter expert) in the entrance criteria process should review assigned areas of responsibility and intensify ongoing efforts to reach unmet goals. Compare demonstrated system performance to required system performance, and compare available resources to required resources. A coherent, complete linkage should extend from system/program requirements down through the planned methods and resources for demonstrating technical and operational performance. Any flaws, inconsistencies, contradictions, voids, or disconnects are potential issues and areas of risk. Accurate and complete inputs are needed from all participants.

X–8. Assessment
The system evaluator, in coordination with the PM and operational tester, should next assess the shortfalls identified in the template review for impacts on the OT program. Per the OTRR agenda depicted in figure 6–7, candid assessments by the evaluator of the system's readiness for OT (the risk of not passing OT) are crucial to the success of the entrance criteria process.

X–9. Standard for judging readiness
Every template and template line item uses the same ideal standard for assessing system readiness for OT and risk level: "Will the system be ready for and successfully complete OT in this area?" The cumulative total of all judgments about these risks will indicate if the complete system is ready for OT. This candid assessment is the heart of the entrance criteria process.

X–10. Development of program goals
PMs must know what events or facts must occur to achieve program goals before OT starts. Empirical, performance-based capability should be developed for each identified deficiency or issue. Satisfaction of demonstrated system performance is the best means to ensure readiness for OT. If possible, make DT more operationally relevant to serve as a predictor of future operational performance. Value judgments backed up by sound technical and military judgment may also be necessary. Areas judged "not ready" will require explanation and an action plan to reach the program goals.

X–11. If standards are not met
Some template line items may not reach the "ideal standard" (for example, are not expected to be ready for OT) after close scrutiny. For example, TMs are often unavailable, produced late, or incomplete at the start of OT. A few unavoidable departures from the ideal standard are expected, yet these areas still require constant, long-term management

attention. Acceptable limitations for certain areas of OT should be discussed. Negotiation of standards and action plans should occur.

X–12. Negotiation

Risk areas persisting after repeated reviews are likely to impact the conduct of OT. Entrance criteria participants must negotiate workaround plans and solutions, or agree to some limitations on OT. The program management office is the focal point for attaining negotiated consensus on managing risks. Workarounds and solutions must be in the best interests of the Army. Operational test officials must be satisfied that the robustness, objectivity, and independence of OT will not be compromised, while the program office must retain sufficient management flexibility to find optimal solutions. Again, sound military and technical judgments are required to reach a corporate Army decision to proceed into OT. Both the system's PM and responsible T&E organization should maintain an appropriate resource management reserve in order to deal with assumed risks and the inevitable surprises associated with any significant T&E effort.

X–13. Reporting

The program management office or other T&E WIPT designated action officer is responsible for consolidating all participants' inputs and observations and preparing the entrance criteria briefing or report. Explicit corrective action plans should be developed for each deficient area.

X–14. Reporting final entrance criteria

The content and format of the templates are discretionary and should be tailored to fit the situation. The final product should be an executive-level review of the entire program conveying enough information for senior leadership to make informed judgments of system readiness for OT. The review must broaden senior leaderships' perspective to the "macro" level where overall program risk is assessed along with supporting details, if required.

X–15. Reporting to certifying officials

After reviewing the briefing or report, the PM will forward it to the OTRR chair who remains responsible for final entrance criteria of system readiness for OT. The PM will brief status of incomplete template action items at OTRR #2 (that is, 60 days prior to start of OT). Representatives from appropriate levels of the using command, OTA, and other participating organizations are required.

X–16. Tailoring the process

As early as practical, the PM, in coordination with the T&E WIPT, should tailor the entrance criteria process to their need for information. The review, assessment, negotiation, and reporting cycle should be repeated as often as necessary.

X–17. Templates not program specific

Since the templates are not program specific, PMs, in coordination with the T&E WIPT, may tailor them to fit specific programs or groups of programs. Some templates may require greater or lesser emphasis depending on the program and its phase of development. The templates allow maximum flexibility in focusing and structuring reviews without losing sight of the original objective—providing an executive-level review of the program.

X–18. Tailoring level of detail

PMs may attach additional information or levels of detail to the templates at their discretion. Some examples might be action plans, requirements thresholds, lists of acquisition regulations and standards, watch lists, breakdowns of specific line items, and points of contact. Additional templates can be developed to cover new areas. On the other hand, aggregation of templates and template line items can reduce redundancy and help managers concentrate on known risk areas. In short, tailor each entrance criteria program to attain the best results.

X–19. Joint and multi-Service programs

This entrance criteria process will be the primary entrance criteria method for all programs when the Army is the lead Service. For programs where the Army is not the lead, the results of this process should flow into the other Service's entrance criteria process.

X–20. Updating the templates

The entrance criteria templates are expected to mature through feedback. Further changes will result from advanced technologies, improved T&E methods, revised acquisition procedures, and restructure of the DoD test infrastructure. All entrance criteria template CBTDEV or FPs should forward their observations and suggested improvements to TEMA. Feedback is essential to keep the process and templates up to date.

Section II

Template Structure

X–21. Interlocking matrix

The templates form a matrix of interlocking subject areas spanning an entire acquisition program. Each template introduces order and reduces risk in a specific segment or aspect of the acquisition program. Some duplication and cross-referencing between templates is necessary because acquisition programs rely on many overlapping disciplines. Decisions about risk in one area often affect other areas. Cross-referencing also facilitates broad area reviews as well as special subject area reviews.

X–22. Consolidation of multiple sources

Each template consolidates as much critical information as possible from multiple sources into a succinct "checklist." Programmatic and regulatory details are left to office of primary responsibility or others more thoroughly conversant with specific acquisition guidance. All information in each template is arranged chronologically as much as possible.

X–23. Answering template line items

Each template contains line items phrased as statements of fact rather than questions. Each line item should elicit a brief summary of program status in that subject area rather than a superficial "yes" or "no" response. The entire group of statements covers the template subject area, but further analysis may be required in certain cases. Line items may be answered individually or in groups depending on how the T&E WIPT has tailored the process. Each template can function as a "tailored checklist" and as a road map for future activities in preparation for OT. As a general rule, aggregation of line items should increase as the review rises up through the chain of command.

X–24. Focus on ends, not means

The templates emphasize "what must be done" rather than "how to do it." No specific problem solving methods are advocated over any other, leaving PMs maximum flexibility to implement their own "best practices." The templates focus on the ends rather than the means.

X–25. Assigning responsibilities

a. A single lead agent, or office of primary responsibility, is suggested for each line item on all templates to assist PMs and other participants in focusing responsibility and increasing accountability for results. Final determination of office of primary responsibility should be assigned as required to improve organizational efficiency, and should be based on who is best suited to complete each task or final product. Note that final approval authority for some line items may lie at higher levels. The suggested office of primary responsibility is a starting point and may vary by program. While other agencies are expected to participate on a collateral basis, multiple office of primary responsibility and offices of collateral responsibility are not listed since responsibility would be defocused, and not all variations between programs can be covered. Once identified and agreed upon, the office of primary responsibility must produce a high quality review in assigned areas and gain the required level of participation from offices of collateral responsibility. The PM, in coordination with the T&E WIPT, is responsible for ensuring that the system is ready for OT.

b. Template legend for figure X–1—

(1) C: Contractor.
(2) CBTDEV: Combat developer.
(3) CTSF: Central Technical Support Facility.
(4) FP: Functional proponent.
(5) OT: Operational tester.
(6) PM: Program/project/product manager.
(7) RTO: Responsible test organization.
(8) SE: System evaluator.

TEMPLATE 1

Test Planning and Documentation

Schedule Template

1. Begin using the OT Entrance Criteria Process as early as possible to help identify all long-lead items and risk areas. (All)

2. Schedule sufficient numbers of entrance criteria reviews using the entrance criteria process. Frequency of reviews should increase as the program nears OTRR #1. (PM)

3. Resolve open issues, particularly with requirements, early enough to permit orderly planning and transition to OT. (PM)

4. Develop realistic, achievable acquisition and test schedules and ensure they are "harmonized" throughout all program documents. Avoid "success oriented" schedules. (PM and OT)

5. Check for congressional and PPBS schedule constraints and incorporate into the acquisition schedule. (PM)

6. Where "concurrent" testing is planned, ensure test planning starts early and that independent operational test objectives are not compromised. (OT)

7. Ensure availability of sufficient and timely RDTE funding and procurement appropriations during each budget cycle to keep the program in technical balance. (PM)

8. Conduct the final entrance criteria briefing a minimum of 30 days (if possible) prior to OTRR #1 to allow sufficient time to address any remaining issues. (PM)

Figure X–1. Schedule operational testing entrance criteria template

TEMPLATE 2

Test Planning And Documentation

Requirements *

1. The MNS must be current and support the latest Defense Planning Guidance (DPG). (CBTDEV/FP)

2. The MNS must be coordinated, validated, and approved at the appropriate levels. (CBTDEV/FP)

3. The MNS mission capabilities must accurately flow down (be linked) through the ORD, AoA, CONOPS, and TEMP to the OT concept and OT plan. (CBTDEV/FP)

4. The system must satisfy projected mission area deficiencies in the MNS and DPG before it is certified ready for OT. (PM)

5. The "strategy-to-task" and "task-to-need" framework in the Mission Area Assessment (MAA), Mission Needs Analysis (MNA), and the MNS must continue to support the preferred solution in the AOA. (CBTDEV/FP)

6. The system must provide the needed capabilities against the most current DIA-validated threat described in the STAR (or STA if a STAR is not available). (PM)

7. Possible joint, multi-national, or multi-Service uses described in the MNS must be addressed during the system's development. (PM)

8. The system must satisfy key constraints and boundary conditions relating to national-level defense planning and support identified in the MNS and DPG. (PM)

9. The ORD system characteristics and capabilities must satisfy each proposed concept in the MNS. (CBTDEV/FP)

10. The ORD must be coordinated and approved at appropriate levels prior to each Milestone, after major program changes, and sufficiently early to develop the OT test concept and plan. (CBTDEV/FP)

11. All capabilities, thresholds and objectives must be stated in operational terms and defined in measurable, beneficial increments of capability. (CBTDEV/FP)

a. Requirements should be stated in such a manner that "testable" MOEs/MOPs can be developed. MOEs must be quantitatively measurable through analytically based evaluation methods when possible. (CBTDEV/FP)

b. A Reliability Correlation Matrix (RCM) must be attached that accurately summarizes the system characteristics and capabilities described in the ORD. The RCM must be up-to-date and in the proper format. (CBTDEV/FP)

Figure X–2. Requirements operational testing entrance criteria template

12. All key performance parameters, (KPP) MOEs, threats, definitions, and other criteria must be consistent (harmonized) between the latest ORD, MNS, STAR, AOA, CONOPS, and APB. (CBTDEV/FP)

13. COICs are crosswalked to the test plan. (OT)

14. High-risk areas and potential problems must be identified prior to start of OT. (CBTDEV/FP)

15. The MATDEV, OT, and all using commands must review changes to the ORD. (CBTDEV/FP)

a. After MS B, the ORD should be modified only due to changes in the MNS or cost-schedule-performance trade-offs conducted during the system development and demonstration phase. (CBTDEV/FP)

b. Changes must be finalized early enough not to have adverse impacts on the successful completion of OT. (CBTDEV/FP)

c. Open requirements issues must be documented and resolved prior to start of OT. (CBTDEV/FP)

d. The ORD and RCM must contain a complete audit trail documenting rationale for all requirements changes, including changes from the APB. (CBTDEV/FP)

16. The C4ISP will capture the system characteristics and capabilities and must satisfy each proposed concept in the MNS/ORD, Joint Tactical Architecture (JTA), and Global Information Grid (GIG) Architecture. (PM)

17. The C4ISP must be coordinated and approved at appropriate levels prior to each Milestone, after major program changes. (PM)

18. The C4ISP CIO Assessment must be completed, submitted to the Army Chief Information Officer (CIO) for approval. (PM)

* Mission Need Statement (MNS), Operational Requirements Document (ORD), and C4I Support Plan (C4ISP)

Figure X–2. Requirements operational testing entrance criteria template—Continued

TEMPLATE 3

Test Planning and Documentation

Analysis of Alternatives (AoA)

1. The AoA (if required) must be updated, validated, and approved at the appropriate level prior to each Milestone. (CBTDEV/FP)

2. All reasonable alternatives must be objectively described. A preferred alternative and its military worth must be clearly identified. (CBTDEV/FP)

a. All relevant costs must be identified using objective engineering and business estimates. (PM)

b. All assumptions and constraints must be explicitly identified and supported by the latest MNS or ORD. (CBTDEV/FP)

c. Acceptable ranges of performance must be established using rigorous cost-benefit, trade-off, and sensitivity analyses to show decision makers at what points certain degradations in system cost or performance yield outcomes that no longer satisfy the mission need. (CBTDEV/FP)

3. Develop MOEs reflecting operational utility and show how they were derived from the MNS. (CBTDEV/FP)

a. MOEs at the operational task level must be "testable and measurable" in order to develop DT and OT test plans and concepts. MOEs must be developed as early as possible and agreed to between CBTDEV/FP and tester. (CBTDEV/FP)

b. MOEs, MOPs, and test criteria must be linked to system performance thresholds stated in the latest MNS and ORD and "track" throughout the program's development. (CBTDEV/FP)

4. As requirements are refined, threats evolve, and tactics change in the ORD, STAR, CONOPS, and maintenance concept (MC), incorporate these changes into the AOA and the OT plan. Ensure all requirements remain "harmonized" and current. (CBTDEV/FP)

5. Describe all databases and M&S assets used in the analysis. Ensure they are up-to-date and have undergone V&V before use in the AOA. In addition, ensure all data bases and M&S assets have undergone VV&A before use in OT. (CBTDEV/FP and OT) (See Template 25–M&S.)

Figure X–3. Analysis of alternatives OT entrance criteria template

TEMPLATE 4

Test Planning and Documentation

System Threat Assessment Report (STAR)

1. The STAR* must remain valid and current with updates made prior to each milestone. (PM)

2. Army must approve the STAR. For ACAT I programs, it must be validated by DIA. (PM)

3. The STAR must be consistent with current DOD projections and "harmonized" with the threats listed in the MNS, ORD, and AOA. (PM)

4. Program objectives from the ORD must be accurately summarized in the STAR. (PM)

5. Sufficient threat detail must be provided to support system R&D and the development of realistic operational mission scenarios in support of the OT plan and schedule. (PM and CBTDEV/FP)

a. All threats must be described in system-specific terms. (PM and CBTDEV/FP)

b. Threat "shot doctrine" and employment tactics must be described. (PM and CBTDEV/FP)

c. The "reactive" threat and potential countermeasures must be described. (PM and CBTDEV/FP)

d. Sources for projections and areas of uncertainty must be cited. (PM and CBTDEV/FP)

* This template refers equally to the System Threat Assessment (STA) as well as the STAR.

Figure X–4. System threat assessment report OT entrance criteria template

TEMPLATE 5

Test Planning and Documentation

Maintenance Concept (MC)

1. The MC must describe the optimal system maintenance strategies, concepts, and methods based on the suitability requirements in the MNS and ORD. (CBTDEV/FP, logistician)

a. The MC must be consistent with the using command's and Army logistics support plans and infrastructure. (CBTDEV/FP and logistician)

b. The system must use an acceptable inter-service, organic, and/or contractor mix. (CBTDEV/FP and logistician)

c. The MC must identify potential high-risk areas and problem areas (such as poor integrated diagnostics, software failures, and data integrity). (CBTDEV/FP and logistician)

d. Limitations and work-around must be identified. (CBTDEV/FP and logistician)

2. Logistics and readiness MOEs, criteria, thresholds, objectives, and definitions in the MNS and ORD must accurately flow down (be linked) to the MC, which must in turn be linked to the OT concept and plan. (CBTDEV/FP and logistician)

3. The strategies and plans in the MC must be sufficiently detailed to support early development of the OT concept and OT plan. (CBTDEV/FP and logistician)

4. Realistic suitability test scenarios for DT must be developed from the MC and be consistent with the CONOPS. (PM)

5. MC must be considered in developing realistic OT test scenarios. (OT and logistician)

6. The MC's strategies and plans for the system will examined in OT. (PM and OT)

a. DT must demonstrate the system is viable and supportable according to the MC and ready for OT. (PM and logistician)

b. The system must demonstrate the capability to satisfy each of the elements of operational suitability and ILS elements found in AR 700-127. (PM and logistician)

c. The system's design must successfully address the quantitative and qualitative constraints identified in the MC. (PM and logistician)

7. System maturity, logistics support, available resources, and personnel must be sufficient to support the MC and maintenance plan during OT. (See Template series under Test Assets and Support) (OT and logistician)

Figure X–5. Maintenance concept OT entrance criteria template

TEMPLATE 6

Test Planning and Documentation

Concept of Operations (CONOPS)

1. The CONOPS must describe optimal system employment methods and tactics and be based on the operational requirements in the latest MNS and ORD. (CBTDEV/FP)

a. CONOPS must be considered in developing the OT concept and OT plan. (OT)

b. The CONOPS must be sufficiently detailed to permit early development of operationally realistic test scenarios and tactics for the OT test concept and test plan. (CBTDEV/FP)

2. Operational effectiveness requirements, criteria, thresholds, objectives, and definitions in the MNS and ORD must accurately flow down (be linked) to the CONOPS, which must in turn be linked to the OT test concept and OT plan. Changes in the MNS, ORD, STAR, AOA, maintenance concept (MC), and TEMP must be analyzed for potential impacts on the CONOPS, which in turn affect the OT plan. (CBTDEV/FP)

3. Realistic test scenarios

a. CONOPS consistency with the MC will be examined in DT. (PM)

b. CONOPS consistency with the MC will be examined in OT. (OT)

4. The system must demonstrate readiness for OT in its intended operational environment using the CONOPS strategies and plans. (PM)

a. The system must clearly demonstrate in DT the potential to perform the roles, missions, and tasks described in the CONOPS. (PM)

b. The system's design must successfully address the quantitative and qualitative constraints identified in the CONOPS that impact system performance in OT. (PM)

Figure X–6. Concept of operations OT entrance criteria template

TEMPLATE 7

Test Planning and Documentation

Test & Evaluation Master Plan (TEMP)

1. The T&E WIPT or other designated forum must review the status of system entrance criteria for OT as directed by the certifying official. (PM)

2. The TEMP must be updated, coordinated, and approved at appropriate levels prior to each MS and after major program changes. (PM)
a. Open issues must be addressed. Changes required by OSD or other decision authorities must be incorporated as agreed. (PM)
b. Coordination must be timely and efficiently planned to minimize chances of late rejection and negative impacts on OT. (PM)

3. The TEMP must be accurately "harmonized" with the most recent ORD and STAR. (PM)

4. The APB and ADM must be reviewed to ensure new directions, requirements, and critical technical parameters are included in the TEMP as appropriate. (PM)

5. The TEMP must establish clear relationships between 1) test management strategy and structure, program schedule, and required resources, and 2) performance requirements, COICs, critical technical parameters (CTPs), evaluation criteria, and MS decision points. (PM)
a. The OT program must be executable in terms of structure, schedule, and resources. (OT)
b. OT test resource shortfalls or limitations potentially impacting OT must be identified and discussed in the TEMP. (SE and OT)
c. Describe the M&S assets to be used in OT. Ensure they undergo VV&A and their use is approved. (See Template 25—M&S) (OT)
d. If LFT is required, include the LFT strategy in the TEMP. (PM)
e. The sources of all technical parameters/requirements must be documented. (PM)

6. The TEMP must describe what DT, OT, or combined DT/OT will do to ensure the system has the potential to meet all CBTDEV/FP requirements. (PM)
a. Show how all critical issues and MOEs will be addressed in OT. (OT)
b. Proposed work-around (to include contractor involvement) must be sound, feasible, and consistent with national policy. (PM)

7. Rationale and provision must be made for any testing deferred past OT into FOT&E and a plan for accomplishment provided. (PM)

8. Requirements/Test Crosswalk Matrix (attachment 1 to TEMP). (PM/OT/CBTDEV)
a. The purpose of the Requirements/Test Crosswalk Matrix is to provide a linkage among the AoAs, MOE, MOS, KPP, COI, and CTP, and then relate these items to specific test events for identification of data necessary to evaluate the system against the requirements. This crosswalk matrix will consist of a foldout spreadsheet or matrix, as shown in appendix D, figure D-2, this pamphlet. (PM/OT/CBTDEV)
b. The linkage can be developed using any one of the categories to generate the association. (PM/OT/CBTDEV)
c. Since the COI are usually the fewest in number, it may be easiest to begin with the COIC and then develop the linkage with the other categories. The MOE/MOS column should reflect precisely the MOE/MOS table contained in Part 1 of the TEMP. The CTP column should also reflect precisely the CTP matrix in Part 1 of the TEMP. (PM/OT/CBTDEV)
d. The second part of the matrix should consist of all test events contained in the test strategy. For each test event, an "x" is placed in a box, provided data from that test will be used to satisfy the corresponding requirement. (PM/OT/CBTDEV)

Figure X–7. TEMP OT entrance criteria template

TEMPLATE 8

Test Planning and Documentation

Operational Test Event Design Plan

1. The OT test concept must be developed and briefed as early as feasible. (OT)
a. The OT concept must describe the characteristics of the operational and maintenance environments and test scenarios the system will encounter in OT. (OT)
b. After OT concept review, the DT program must be made sufficiently rigorous to ensure CBTDEV/FP requirements can be met or exceeded in these environments. (PM)
c. Ensure T&E WIPT meetings are scheduled and structured to add value to the OT through better MS reviews and entrance criteria briefings. (PM)

2. The OT Event Design Plan (EDP) must be developed and coordinated as early as feasible at appropriate levels. If an OSD T&E oversight program, OSD/DOT&E approval of test plan adequacy is required. (OT)
a. Prior to T-120 days the OT EDP must be provided to review and approve the plan. (OT)
b. Does the Baseline Correlation Matrix (BCM) and its MOEs/MOPs have clearly defined links with the MNS and ORD (SE).

3. A phase of rigorous, OT must be planned with sound T&E methodologies evident throughout. (OT)
a. Sufficiently realistic testing must be planned under the specified operational environment from the OMS/MP and other documents. (OT)
b. Open issues and disconnects (such as with test methodologies, requirements, and MOEs) must be resolved. (OT)
c. Definitions, formulas, models, scenarios, and evaluation criteria must be standardized as much as possible between the DT and OT plans. (OT)
d. M&S assets planned for OT should be as consistent as possible with the M&S assets used in the AOA and the DT. (See Template 25—M&S) (OT)

4. All resource requirements in the Outline Test Plan (OTP) (M&S support, test articles, training, fault analysis and, contracting) must be identified. (See Template series under Test Assets and Support.) (OT)

5. A program with combined DT/OT must ensure the following:
a. None of the DT or OT test objectives are compromised as a result of joint/combined testing. (OT)
b. DT data and formats are useable in OT as much as possible. (OT)
c. Test item configurations are rigorously controlled according to plan. (See Template 11—Configuration Management Plan.) (PM)
d. Duplication and gaps in testing are minimized. (OT)
e. A prudent number of backup resources (test assets and funds) are available to supplement OT if planned DT data is unusable or unavailable. (PM)

6. Describe all OT test limitations for example, lack of test resources, time, system capabilities, insufficient realism that may impact the Milestone C decision. (OT)
a. Describe how these test limitations will be addressed in FOT&E and beyond. (OT)
b. Detailed test procedures must be developed and provided to the PM. Test procedures should be dry run. (OT)

Figure X–8. OT Event design plan entrance criteria template

TEMPLATE 9

Test Planning and Documentation

Deficiency Identification and Correction Process

1. A contractor-owed and contractor-based deficiency reporting system must be established and provide useable information and inputs to the Government's deficiency reporting system. (C)

2. A Government-run deficiency reporting system must be established for promptly identifying and accurately reporting system/materiel deficiencies. (PM)

3. When, during testing, test incident reports identify materiel/system deficiencies the information should be utilized and inputted to the deficiency reporting system. (RTO)

4. A review board must ensure that disposition instructions are provided to resolve all deficiency reports and list the impacts to operational testing. (PM)

5. A review board will review, validate, and prioritize all deficiency reports in a manner that is timely and responsive. (PM)

6. A failure reporting and corrective action system or similar system must be established. It will be used as a closed-loop process for identifying and tracking root failure causes including design errors, part problems, workmanship defects and/or process errors, and subsequently determining, implementing, and verifying an effective corrective action to eliminate their re-occurrence. (PM)

7. Reliability, availability, and maintainability (RAM) scoring and assessment conferences will be established to review all RAM data and to develop the procedures to be utilized for the conferences. (SE)

8. Assure the contractor and the T&E WIPT has been apprised as to the level of involvement and participation the contractor will have in the scoring/assessment conferences. (PM)

9. Any remaining deficiencies that remain open from developmental testing and are still being considered for corrective actions or requiring disposition instructions must not preclude the successful conduct of operational testing and the evaluation or assessment of the achievement of operational requirements. (PM)

Figure X–9. Deficiency identification and correction process OT entrance criteria template

TEMPLATE 10

Test Planning and Documentation

Security Planning

1. Identify security constraints and their impacts on OT. Develop work arounds where possible. (OT)

2. The system operations security (OPSEC) plan must be current and systems engineering security requirements accomplished. (PM)

a. Identify and resolve any disconnects between service and system Security Classification Guides (SCG). (PM)

b. Ensure secure communications and/or frequencies (if required) are in place to support system-level DT and OT. (PM or OT)

c. Ensure data encryption and encoding devices are available (if required). (PM)

d. Ensure security measures and requirements (such as, telecommunications electronics materiel protection from emanating spurious transmissions (TEMPEST) and high-altitude electromagnetic pulse {HEMP}) are accomplished and current. (PM)

e. Ensure test ranges or facilities have security planning, procedures, and personnel documented, in-place, and implemented. (OT)

3. The system's SCG and Program Protection Plan must be current. Ensure computer system security protection measures are accomplished and current. (PM)

4. Security clearances and required security training for test team personnel must support the OT plan and schedule. (OT)

Figure X–10. Security planning OT entrance criteria template

TEMPLATE 11

Test Planning and Documentation

Configuration Management (CM) Plan

1. A system configuration control mechanism must be in place for all system components and support items (for example, hardware, software, support equipment, and GFE). (PM) (See Template 17—Production Representative Articles.)

a. A Configuration Management Plan and configuration baselines must be used to ensure an orderly transition from one MS decision point to the next. (PM)

b. The Government must have sufficient control or oversight over the configuration to ensure the results of OT are not invalidated. (PM)

2. The exact system configuration must be traceable throughout the program. The PM must also ensure that the capability exists to assess any configuration differences between pre-production and production test articles. (PM)

3. If known deficiencies remain in test articles before start of OT, the Configuration Management Plan must describe strategies for managing the following areas: (See Template 21—Deficiency Resolution.)

a. System form, fit, and function must not be adversely affected as a result of each deficiency. (PM)

b. The impacts of fixing before versus after OT must be assessed. (PM)

c. Additional testing needed to verify correction of deficiencies must be identified. (PM)

d. The system configuration will be stable and production representative before the start of OT. (PM)

4. Identify in the plan any system development or maturity issues that negatively impact the OT plan and schedule in support of the next milestone review. (PM)

5. Certify that the start of full-rate production will not invalidate OT results due to changes in or termination of any quality control procedures or mechanisms (such as environmental stress screening) used during pre-production. (PM)

Figure X–11. Configuration management plan OT entrance criteria template

TEMPLATE 12

System Design and Performance

Contractor Testing

1. Ensure all system specifications and contractor requirements reflect the latest ORD changes. Late ORD changes may not be practical to reflect in the system spec. (PM)

2. A comprehensive test plan for contractor development, qualification, and production acceptance testing must be in place. (C)

a. The plan must minimize overlaps and gaps and collect maximum information from every test event. (C)

b. Requirements and specifications must flow down accurately and clearly from prime contractors to subcontractors. (C)

c. Test methods selected must determine if all aspects of the capabilities, performance-based specification and CBTDEV/FP requirements can be met. (C)

d. Multiple test events should be performed under varying conditions to demonstrate specification compliance. (C)

e. Sub-system and system pass/fail specification thresholds must be directly traceable to the stated operational capabilities in the latest ORD. (PM)

f. A realistic (attainable) event-driven test schedule must be proposed and funded. (C)

3. Contractor testing must demonstrate that the system and/or components are performing as planned at each step in development. Government engineering analysis should determine if test results support achievement of the spec and if the system is projected to meet operational requirements. (PM and C)

4. Ensure contractor personnel will not be involved in OT except where permitted by law. (See Template 29—Support Agreements and Support Contractors.) (OT)

5. Periodic reviews should be made of available government facilities with the goal of using them in contractor testing wherever cost-effective and feasible. (PM)

6. A deficiency identification, tracking, and correction system must be in place to monitor test failures. (See Template 9—Deficiency ID and Correction Process.) (C)

a. All test failures and resultant system design changes must be documented and analyzed. Tests must be repeated as necessary to verify specification compliance. (C)

b. Document all changes to specification threshold (pass/fail) values and rationale. (PM)

c. Government review must continually monitor for impacts on DT and OT. (PM)

7. Planned contractor testing must be completed according to the contract specification before government acceptance and OT. Contractor testing deferred past government acceptance of the system should be documented and approved in the TEMP. Impacts to DT and OT must be documented. (PM and C)

Figure X–12. Contractor testing OT entrance criteria template

TEMPLATE 13

System Design and Performance

Developmental Testing (DT)

1. System requirements in the ORD must accurately flow down through the contract specifications and be demonstrated during DT. (PM)

2. When design-cost-performance trade-offs are made that may not meet CBTDEV/FP requirements/capabilities, CBTDEV/FP concurrence must be obtained and documented. (CBTDEV/FP must document in ORD and RCM.) (PM)

3. The DT schedule and testing must be planned and executed to allow sufficient time to certify system readiness for OT, start OT, and complete OT before MS C. (PM and OT)
a. DT must demonstrate that system design is complete and acquisition risks have been minimized. (PM)
b. DT must validate that contractor testing is complete, or that a plan exists to finish testing. (See Template 12—Contractor Testing.) (PM)
c. The results of DT indicate the system will perform successfully in OT and will meet MS C approval criteria. All specified technical thresholds have been met. (RTO)
d. Sufficient suitability tests must be conducted to permit credible predictions about RAM. All suitability thresholds have been assessed as achievable. (RTO)

4. A government-run DR system must be in place in support of DT and OT for identifying, tracking, and reporting deficiencies. (PM) (See Template 9—Deficiency ID &Correction Process.)

5. The government must be in control of a system configuration tracking and control process during DT that will support OT. The system design must be finalized with no major changes planned prior to OT. (See Template 17—Production Representative Articles) (PM)

6. Sufficient operationally relevant DT must be done, culminating in a "dress rehearsal" in the final phase of test, to determine if operational requirements can be met before OT. Sufficient interoperability and compatibility testing with other systems must be done. (See Template 18—Interoperability and Compatibility.) (PM and RTO)

7. LFT (if required) must be complete before start of OT, or a waiver approved prior to MS B. (See Template 14—Live Fire Testing.) (PM)

9. For combined T&E, minimize duplication and gaps in testing and the use of facilities. Data formats used in DT and OT must be compatible to maximize availability and usability of data. (See Template 8—OT Event Design Plan.) (OT)

10. An agreed-upon plan and rationale must exist (for example, in the TEMP) for testing any areas or capabilities deferred past the start of OT. If there are any incomplete test areas, explain why and give impacts on OT. (PM and RTO)

11. Ensure sufficient interim DT results and conclusions are available to support entrance criteria of readiness for OT. (RTO)

Figure X–13. Developmental testing OT entrance criteria template

TEMPLATE 14

System Design and Performance

Live Fire Testing (LFT)

1. Per the annual OSD T&E Oversight List, determine if the program is a live fire covered system. Review the most current requirements, threats, and operational scenarios in the MNS, ORD, STAR to determine if the system is a "covered system." OSD concurrence is required. (PM)

2. If LFT is required (for a covered system), it must be completed before start of OT or a LFT waiver approved before Milestone B. (PM)

3. If LFT is required, determine LFT scope and complete a cost-benefit analysis. (PM)

a. If LFT is determined to be cost-effective and will be accomplished, include a LFT strategy in the TEMP and prepare a LFT plan for OSD comments. (PM)

b. Provide a LFT report to OSD for comments and before entrance criteria for OT. (PM)

4. If LFT is determined not to be cost effective, prepare a LFT waiver request package with an alternate plan for vulnerability/lethality testing for HQ ARMY and OSD approval before Milestone B (PM)

a. Include the alternate vulnerability/lethality testing strategy in the TEMP. (PM)

b. Provide the alternate plan to OSD for comments. (PM)

c. Provide a vulnerability/lethality test report to OSD for comments and before entrance criteria for OT. (PM)

5. Deficiencies identified during LFT that are to be corrected must be tracked and retested prior to entrance criteria for OT. (PM)

6. Fully comply with all system-specific congressional direction regarding LFT. (PM)

Figure X–14. Live fire testing OT entrance criteria template

TEMPLATE 15

System Design and Performance

System Performance

1. The system must demonstrate credible potential of meeting operational effectiveness and suitability requirements in its intended operational environment using operationally relevant scenarios. (PM)

a. The system must demonstrate that it has credible potential to perform successfully in OT (meet CBTDEV/FP requirements) and will meet Milestone C approval criteria. (PM)

b. Areas of system effectiveness and suitability must be reviewed against requirements (MOEs, MOPs, thresholds, objectives, and other test criteria). (PM)

2. System T&E must demonstrate that known design problems have been corrected or resolved. (See Template 21—Deficiency Resolution.) (PM)

a. Any remaining problem areas must have minimal impact on the outcome of OT. (PM)

b. Fixes must be identified for all problems deferred past the start of OT into FOT&E. (PM)

3. Is the software sufficiently mature to ensure acceptable hardware and software integration. (PM)

4. System integration problems must be corrected to allow operators to satisfy mission requirements. The system must be ready for system or mission-level testing. Integration among system components and subsystems must optimize total system design and performance capabilities. (PM)

5. If planned certification of the system is to occur in increments of increasing capability (maturity), describe what capabilities are lacking at this time. (PM)

6. LFT (if required) must be complete and achieve required (acceptable) levels of system survivability or lethality. (See Template 14—Live Fire Testing.) (PM)

Figure X–15. System performance OT entrance criteria template

TEMPLATE 16

System Design and Performance

System Maturity

1. Interim (block, P3I, evolutionary) as well as final objective requirements for system and sub-system components (to include support equipment) should be stated in the ORD and reliability centered maintenance. Target dates for these maturity levels should be provided. (CBTDEV/FP)

2. Interim values for system and sub-system level components (to include support equipment) might be available and transferred into the performance-based specification. (PM)

a. A reliability growth plan must be developed and coordinated. (PM)

b. Identify any system development and/or maturity aspects impacting the ability to start and complete OT in time to support Milestone C. (PM)

3. The system's development progress must adhere to any specified interim and/or mature values and schedules. (PM)

a. DT must demonstrate the system is on track (expected to meet interim and/or mature values at the specified maturity levels) to be certified ready for OT. (PM)

b. Any constraints precluding the system from meeting interim and/or mature requirements during OT must be assessed. (PM)

4. System configuration to include software maturity must be carefully controlled as the system matures. Identify differences between the OT configuration and the production configuration, to include an assessment of potential impacts on the validity of OT. (See Template 11—Configuration Management Plan.) (PM)

5. Efforts should be made to improve hardware/software problem identification and isolation and increase the accuracy of determining problems with less incidents of false indications of problems. (PM)

Figure X–16. System maturity OT entrance criteria template

TEMPLATE 17

System Design and Performance

Production Representative Articles

1. Articles (to include support equipment, software, GFE) must be as production-representative as possible and available in the required quantities to support the OT plan and schedule. (PM)

2. A system configuration control mechanism must be in place for all system components and support items (for example, hardware, software, support equipment, and GFE). (PM)

a. The Government must have sufficient control or oversight over the configuration to ensure the results of OT are not invalidated.) (See Template 11—Configuration Management Plan.) (PM)

b. The exact system configuration must be traceable throughout the program. (PM)

3. Ensure the design is compatible with factory production procedures. (PM)

4. If known deficiencies remain in test articles (See Template 21—Deficiency Resolution.) —

a. Certify how form, fit & function are affected as a result of each deficiency. (PM)

b. Assess the impacts of fixing before versus after OT. (PM)

c. Identify additional testing needed to verify correction of deficiencies. (PM, SE, and OT)

5. Certify that the start of rate production will not invalidate OT results due to changes in or termination of any quality control procedures or mechanisms (such as environmental stress screening) used during pre-production. (PM)

6. Identify any system development or system maturity issues that negatively impact the OT plan and schedule or support the next MS review. (PM)

7. Other systems and subsystems required to interoperate with the test articles (including external systems) must be available to permit testing in an operationally realistic manner. (OT)

a. A process must be in place to manage system integration with other required systems and subsystems. (PM)

b. Ensure embedded test instrumentation is "invisible" to system performance and operators. (PM)

Figure X–17. Production representative articles OT entrance criteria template

TEMPLATE 18

System Design and Performance

Interoperability & Compatibility

1. The system must be interoperable and compatible with other systems as required in the MNS, ORD, and/or by DISA. (PM)

a. The system's performance must not be degraded when operated with other systems during OT and in the intended operational environment. Likewise, the system must not degrade the performance characteristics of other systems beyond the limits stated in the ORD. (PM)

b. Quantify how much degradation (or enhancement) will result in other interoperable systems' performance characteristics when the system is deployed. (PM)

2. Data passed to and from other independent and interoperable systems must be compatible. (PM)

3. For C4I systems (most are considered joint)—

a. Interface control documents are needed with affected agencies to establish data exchange formats, and communication protocols. (PM)

b. Check for status of Tactical Data Link (TDL), United Stated Message Text Format (USMTF) & Variable Message Format (VMF) and standards interoperability). (PM)

c. Obtain DISA and JITC joint interoperability entrance criteria as required. (PM)

4. Ensure compliance with the Army Electromagnetic Compatibility Program and Radio Frequency Spectrum Management guidelines. Assistance available at EPG and HQDA CIO Spectrum Directorate. (PM)

5. Conduct intra-Army, interoperability testing at CTSF and receive CIO/G6 interoperability and compatibility certification. (PM)

6. Other systems and subsystems required to interoperate with the test articles (including external systems) must be available to permit testing in an operationally realistic manner. (OT)

a. A process must be in place to manage system integration with other required systems and subsystems. (PM)

b. Ensure embedded test instrumentation is non-intrusive to system performance and operators. (PM)

Figure X–18. Interoperability and compatibility OT entrance criteria template

TEMPLATE 19

System Design and Performance

Software Development

1. System functionality and maturity must be developmentally tested at the system level prior to the start of OT. (PM)

2. Define software-related exit criteria at MS B. These criteria may be modified and/or criteria added as appropriate during system development. (PM)

3. Develop and implement a "requirements traceability" metric to measure the adherence of the software products (to include design and code) to the ORD requirements (for S/W Blocking functionality). (PM)

4. System level integration testing of software and hardware-software-firmware interfaces must be monitored, documented, and complete. (PM)

5. Ensure interoperability requirements are met by verifying software interfaces are operational. The software must be tested at the unit, integration, and system levels, and if the software is modified, adequate regression testing must be done. (See Template 18—Interoperability and Compatibility) (PM))

6. Known software and firmware discrepancies affecting system performance or the OT must be properly documented and appropriate corrective action(s) taken. (PM)

7. Sufficient regression testing must be done at the unit, integration, and system levels to ensure any changes do not result in additional defects. (PM)

8. Ensure the Government has an effective software configuration management and control system and control procedure in place. (See Template 11—Configuration Management Plan) (PM)

9. Software manuals (Software CBTDEV/FP's Manual(s), Software Programmer's Manual, Computer System Operator's Manual, Firmware Support Manual, and Computer System Diagnostic Manual) must be validated and up-to-date with the current software blocking baseline. They must be sufficient to support OT. (PM)

10. Software baseline configurations and firmware configurations must be fully documented and "frozen" before starting OT. No unilateral decision to make software changes will occur after OTRR #2. (PM and OT)

11. The software must be stable (operate error free for a reasonable length of time prior to OT). (PM)

12. The software must be certified (security, flight safety, and nuclear weapons) for operational use as appropriate. (PM)

13. Government facilities, tools, and manpower must adequately support fielding of the software if the MC requires the Government to maintain the software. (PM)

14. Contractor software support (if required for the fielded system) must be representative and available to support the OT plan and schedule. (PM)

Figure X–19. Software development OT entrance criteria template

TEMPLATE 20

System Design and Performance

Safety Reviews and Certifications

1. The system must be capable of being safely operated and maintained during OT and in its intended operational environment. (PM)

2. All catastrophic and critical hazards (Category I and II) must be addressed through the Safety Review Board and closed before the start of OT. (PM)

a. The CONOPS and MC must be reviewed, and safety constraints and limitations addressed. (PM)

b. Perform a Health Hazard Assessment to minimize risks during OT. (PM)

c. Review OSHA, State, and Army hazardous waste regulations for compliance. (PM)

d. Environmental impacts must be identified, mitigated, or neutralized. (PM)

3. Validated technical, safety, and procedural manuals must be available to support the OT plan and schedule. (PM)

4. Operator and maintenance personnel must have safety training completed in time to support the OT plan and schedule. (OT)

5. Formal entrance criteria for OT may be required from the following boards (PM) -

- Non-nuclear Munitions Safety Board
- Conventional Munitions Board
- Flight Safety Board
- Airframe Entrance criteria
- Range Safety
- Directorate of Nuclear Safety

6. Obtain operational flight waivers for systems requiring safety/flight release from aircraft. (OT)

Figure X–20. Safety reviews and certifications OT entrance criteria template

TEMPLATE 21

System Design and Performance

Deficiency Resolution

1. All deficiencies must be promptly and accurately reported and tracked. (PM)

2. Known deficiencies or capabilities deferred past the start of OT must be reviewed and prioritized by a DR review board and an impact analysis performed. (PM)

a. Category I and II deficiencies having impacts on OT or any COI must be fixed and closure verified according to an agreed upon plan. (PM)

b. Ensure OT can be completed as planned and results will not be invalidated due to deferred deficiencies. (PM)

c. Assess any synergistic relationships between deficiencies for impact on OT. (PM)

d. Deficiencies should be rank-ordered, and the most critical worked first or as agreed to by the CBTDEV/FP(s) and RTO(s). (PM)

e. CBTDEV/FP and RTO concurrence is required in the rank ordering. (CBTDEV/FP)

3. The deficiency analysis process must be complete and coordinated with CBTDEV/FP and testers prior to the start of OT. (PM)

4. If some deficiencies cannot be corrected or resolved prior to start of OT, develop a plan for testing deferred capabilities and fixes after OT is done. Define the scope and content of software and hardware releases planned after completion of OT. (PM)

5. System form, fit, and function must not be affected if OT is conducted with any known deficiencies. (See Template 17—Production Representative Articles.) (PM)

Figure X–21. Deficiency resolution OT entrance criteria template

TEMPLATE 22

Test Assets and Support

Test Team Training

1. OT test team training requirements and assets must be identified early and in sufficient detail. For joint and combined systems, additional joint/combined training requirements must be identified. (OT)

2. Required training must be adequately contracted for, funded, and scheduled to assure completion at the times required in the OT plan and schedule. (PM and OT)

a. Software maintenance training must be completed for OT evaluators if the software maintenance concept is for the Government to maintain the software. (PM)

b. OT test player personnel must be certified proficient in their respective skills before the start of OT. (OT)

c. Training must include normal and emergency operations to operate and maintain the system(s) according to the CONOPS and MC. (PM)

3. Exercise all test procedures in a pilot test, to include an end to end data run, before start of OT. (OT)

Figure X–22. Test team training OT entrance criteria template

TEMPLATE 23

Test Assets and Support

Personnel

1. Identify OT test player personnel requirements, including software maintenance skills and security clearances. Number of personnel and skill levels must be representative of the field (reflect the operational environment). (OT)

2. Written procedures must be available for test team personnel. (OT)

3. Written agreements must be in place establishing the sources for required personnel. (OT)

4. Estimates of maintenance requirements (in terms of person hours and personnel) for LRUs, subsystems, and the full system must be available. (PM)

5. Contractor support (ICS and CLS) must be identified.* (PM)

6. Required training must be completed or scheduled for completion to support the OT plan and schedule. (See Template 22—Test Team Training.) (PM)

* ICS Integrated Contractor Support
CLS Contractor Logistical Support

Figure X–23. Personnel OT entrance criteria template

TEMPLATE 24

Test Assets and Support

T&E Infrastructure

1. Resources and funding must be approved to start and sustain a credible OT program. (PM)

2. Test ranges (both indoor and outdoor) and other test facilities must be properly equipped, manned, funded, scheduled, and personnel briefed before start of OT. (OT)

3. Realistic targets (or validated target simulators) must be in the most current operational configuration(s) and available in sufficient quantities. (PM and OT)

4. Sufficient threat densities, either in open-air or indoor facilities, must rigorously stress the system in as realistic a combat environment as possible. (See Template 4—STAR and Template 30—Threat Systems.) (OT)

5. Adequate test instrumentation and data reduction capabilities must be identified, funded, scheduled, and support agreements negotiated on use rates and data requirements. (OT)

6. Modeling and simulation assets (including simulators, test drivers, and scenarios) must be VV&A scheduled, and available to support the OT plan and schedule. (OT)

7. Use the appropriate "test process" (that is, EC Test Process) if available. (PM and DT)

8. Identify T&E infrastructure shortfalls in the TEMP and inform Army TEMA. (PM)

9. An EIS (if required) addressing all Federal, State, Army, and local restrictions must be completed and approved, or waivers granted. (RTO)

Figure X–24. T&E infrastructure OT entrance criteria template

TEMPLATE 25

Test Assets and Support

Modeling and Simulation (M&S)

1. Develop an M&S plan for the system linking M&S requirements throughout the program (from the AOA through the Milestone C decision). (PM)

a. Show how proposed M&S resources support the program by linking them directly to requirements and the AOA. (PM)

b. M&S requirements, including interfaces with other systems, must be identified and included in the TEMP. (PM)

c. M&S assets should be usable by both the DT and OT test teams. The OT team should receive adequate training in their use. (PM)

d. Definitions, formulas, and evaluation criteria used to determine operational effectiveness and suitability must be consistent between DT and OT. (OT)

e. The system's M&S support requirements (to include the system life cycle) must be identified as early as possible. A life cycle plan must be developed for ownership and maintenance of M&S assets after system deployment. (PM)

2. An M&S VV&A plan must be developed with a comprehensive schedule that supports the OT plan and schedule. (OT)

a. Scenarios, test tools, and analysis tools required for testing must be adequately documented. (PM)

b. M&S assets must be VV&A independently of the developer and CBTDEV/FP before use in OT. Key assumptions (threats and tactics) must also be VV&A. (OT)

c. The design engineering notebook data must be reviewed. Physics models can be V&V, whereas operations analyses are subjectively V&V. Empirical test data should be used to establish model credibility. (PM)

d. The correct M&S accreditation agent must be used. (OT)

3. Establish M&S documentation and audit trail. (PM)

4. If M&S will generate results used to support or influence major decisions, OSD/DOT&E must approve their use in OT. (OT)

Figure X–25. Modeling and simulation OT entrance criteria template

TEMPLATE 26

Test Assets and Support

Support Equipment

1. Peculiar, common, and unique* support equipment (SE) must be identified as early as feasible. (PM)

2. Peculiar SE and its required support (technical data, spares, etc) must meet the maintenance times and capabilities stated in the ORD. (See Template 15— System Performance.) (PM)

a. Peculiar SE must be available in required quantities to support the OT plan and schedule. (PM)

b. Peculiar software SE and its supporting technical data, compilers, manuals, etc., must be available if the Government maintains the software. (PM)

3. Peculiar SE must be in production representative configurations and fully interoperable and compatible with the system(s) it supports. (See Template 17—Production Representative Articles.) (PM)

a. Assess any configuration differences between pre-production and production peculiar SE and the expected impact on the validity of OT. (PM)

b. The Government must have positive control or oversight over SE configurations. (PM)

4. Common SE must be identified and available in the required quantities to support the OT plan and schedule. (CBTDEV/FP)

5. Unique SE must be identified and available in the required quantities to support the OT plan and schedule. (PM)

6. SE training must be accomplished or scheduled to support the OT plan and schedule. (PM)

* **Peculiar SE.** SE under development in support of the system being tested.
Common SE. Fielded SE that supports existing systems used in OT.
Unique SE. Contractor or Government furnished SE for RDT use only.

Figure X–26. Support equipment OT entrance criteria template

TEMPLATE 27

Test Assets and Support

Sufficiency of Spares

1. Sufficient spares must be available to support test assets, test scenarios, and SE according to the OT plan and schedule. Support levels must be based on the total number of expected operating test hours. (PM)

2. Spares repair procedures and capabilities (for blue suit and/or CLS, if required) must be in place to support the OT plan and schedule. (PM)

3. Provision must be made for timely failure confirmation and repair action reports to the OT test team. (PM)

4. The management concepts for primary operating stocks, war readiness spares support, and for battle damage repair must be estimated prior to OT plan development. (PM)

5. Candidate spares for maintenance concept must be identified. (PM)

6. An Integrated Logistics Support Plan (ILSP) must be developed which accurately reflects the maintenance concept and CONOPS. (PM)

a. Identify the risks and limitations in the spares which support OT. For spares with limited availability, define how quickly they must be replenished. (PM)

b. The projected number of spares and rates of replenishment must support the operations tempo of the OT. (PM)

7. Validate that a successful Logistics Demonstration was conducted which verified that the training material, level of maintenance, sparing concept, repair/replacement criteria had been met by the system. (PM)

Figure X–27. Sufficiency of spares OT entrance criteria template

TEMPLATE 28

Test Assets and Support

Packaging, Handling, and Transportation

1. Shipping containers, packaging, handling, and transportation components and methods must be fully qualified and expected to meet the requirements stated in the ORD. Operationally representative maintenance demonstration scenarios must be used. (PM)

2. Adequate numbers of production representative shipping containers and packaging must be used to transport all test articles to the OT sites. (PM)

3. TOs must be validated and available to support the OT plan and schedule. (PM)

4. Shipping, transportation, receiving, and storage arrangements must be in place with the contractor and host base transportation offices to ensure timely shipping, receiving, and resource protection of test and support assets. (OT)

5. OT test player maintenance personnel must be adequately trained. (See Template 22—Test Team Training.) (PM)

Figure X–28. Packaging, handling, and transportation OT entrance criteria template

TEMPLATE 29

Test Assets and Support

Support Agreements and Support Contractors

1. MOUs and MOAs should establish the availability of test and support resources needed to support the OT plan and schedule. (OT)

2. For multi-Service testing, comply with the terms of the "MOA on Multi-service Operational Test and Evaluation and Joint Test and Evaluation (MOT)." (OT)

3. Host base support agreements should be established for using required ranges, test facilities, airspace, frequencies, etc., and base support functions such as supply, transportation, and billeting. (OT)

4. Necessary support agreements should be established with other Government agencies for such functions as data processing, failure analysis, communications, and security. (OT)

5. The potential for conflict of interest must be strictly avoided, mitigated, or neutralized before any contractor is allowed to participate in the support of OT. (OT)

6. All contractor assistance or services required to support OT must be identified in the OT event design test plan and TEMP. (Some types of contractor involvement are prohibited by public law.) (OT)

7. The potential for conflict of interest must be strictly avoided, mitigated, or neutralized before any contractor is allowed to participate in the support of OT. (OT)

8. System contractor report generation procedures must be established for depot-level repair and maintenance actions. (PM)

9. Support contractor services must be established for any required data collection, reduction, and analysis capabilities needed in OT that are not performed by green suiters. (OT)

Figure X–29. Support agreements and support contractors OT entrance criteria template

TEMPLATE 30

Test Assets and Support

Threat Systems

1. Test threat "shot doctrine" and employment tactics must be correlated to the CONOPS and the STAR. (See Template 4–STAR.) (PM)

2. Test threat "shot doctrine" and employment tactics must be correlated to the CONOPS and the Test threat systems and related support required for OT, including M&S assets, must be identified and programmed as early as possible. (OT)

3. Test threat "shot doctrine" and employment tactics must be correlated to the CONOPS and the Test threat systems and M&S assets must be undergo VV&A before use in OT. (See Template 25—M&S.) (OT)

4. Test threat "shot doctrine" and employment tactics must be correlated to the CONOPS and identify known system limitations and voids in covering the threat spectrum. (PM)

a. The system must demonstrate credible potential to meet the required capabilities against the threats described in the ORD and STAR. (PM)

b. If the system will be certified in increments of increasing capability, describe what capabilities are lacking at this time. (PM)

c. Develop a comprehensive plan for dealing with system capabilities deferred past OT into FOT&E. (PM)

d. Identify known test threat limitations and voids in covering the threat spectrum. (SE and OT)

e. Where limitations exist in test threat systems used for OT, obtain approval to fill gaps with facility testing and M&S. (PM)

5. Sufficient threat densities must rigorously stress the system in an operationally relevant combat environment. (See Template 24—T&E Infrastructure.) (PM)

6. Develop a data reduction and correlation plan for using all valid threat testing data. (PM)

Figure X–30. Threat systems OT entrance criteria template

TEMPLATE 31

Test Assets and Support

Technical Data

1. Operator and maintainer technical data must be available to support the OT plan and schedule and be acceptable to the OT test director. (PM)

a. Technical Orders (TOs) from other interoperable systems (hardware, software, and GFE) must be available to support the OT plan and schedule. (PM)

b. Technical data required to evaluate system suitability and software supportability (includes engineering drawings, lists, specifications, standards, process sheets, manuals, technical reports, catalog items, documentation of computer programs and related software) must be available to support the OT plan and schedule. (PM)

2. TOs must be validated prior to use in OT. (PM)

3. A Technical Order management activity must be in place to manage TO deliveries, changes, and other TO requirements. Procedures must be established to process changes to technical data and TOs. (PM)

Figure X–31. Technical data OT entrance criteria template

TEMPLATE 32

Test Assets and Support

Central Technical Support Facility (CTSF)

1. Intra-Army interoperability certification applies to all Army operational-through tactical-level C4I systems prior to release to the field, regardless of the acquisition category. Communications/data interfaces testing in support of intra-Army interoperability certification will be addressed in OTRRs and considered entrance criteria prior to decision reviews, operational testing, and materiel release. (CIO/G-6)

2. Establish CTSF testing timelines for intra-Army certification. (CTSF)

a. Initial Coordination & System Identification - Initial contact from system representative requesting certification testing. (TSM or PM)

b. Initial Coordination Meeting - The system's representative: identifies issues, tours facility, and identifies and coordinates for special equipment. (PM)

c. Test schedule will slip if the following requirements are not met:

(1) PM submits certification funds to CTSF IAW the instructions in chapter 4. (PM)

(2) The CTSF begins development of the test plan that will outline basic architecture requirements, required systems interfaces; base test cases, funding restrictions and other pertinent data. (CTSF)

d. Test Report delivered to CIO/G6. The final Test Data Report, signed by the CTSF Technical Director, Test Cell Director, and the Test Officer will be sent to CIO/G6. CIO/G6 will notify the system's TSM/PM of their certification status. (CTSF)

Figure X–32. Central test support facility OT entrance criteria template

TEMPLATE 33

Test Assets and Support

Joint Interoperability Testing

Under the provisions of DoD Directive 4630.5, "all C4I systems developed for use by US forces are considered to be for joint use." The Joint Chiefs of Staff have published the TADIL-A/B/J and USMTF standards that are designed to ensure systems meet end users information exchange needs as well as their interoperability requirements. Program Milestone C decisions now depend on joint interoperability testing and certification from the Joint Interoperability Test Command (JITC). The USA CECOM Software Engineering Center serves as the Army Participating Test Unit (APTU), and is responsible for the overall coordination of Army systems to be tested/certified by the JITC.

The following steps are followed by the JITC during joint system testing and certification:

1. PMs will afford JITC the opportunity to review applicable system documentation to include–

a. Mission Need Statement - used early during program development to identify high level interoperability requirements. (PM)

b. Capstone Requirements Document - provides the overarching view for Family-of-Systems/System-of-Systems. This is used by JITC to determine interoperability requirements with external systems. (PM)

c. Operational Requirements Document - includes the interoperability requirements (KPPs) and joint top level information exchange requirements (IERs) as defined by CJCSI 3170.01 and CJCSI 6212.01. (PM)

d. C4I Support Plan - This identifies C4 intelligence, surveillance, and reconnaissance infrastructure support and system interface requirements. (PM)

e. TEMP - The TEMP is used to determine the scope and manner that system interfaces will be examined during the testing process. Identify in the TEMP required CTPs and COIs that address interoperability. (PM)

2. Development Test - The PM will work with JITC to ensure that the system conforms to the JTA-A or other applicable standards. (PM)

3. Operational Test - JITC will work with the Operational Test Agency (OTA) to ensure adequate interoperability testing is accomplished and suitable data is provided to the JITC for evaluation. Interoperability evaluations will continue throughout the entire life cycle of each system. Based on DT, JITC will provide a recommendation as to whether a system is ready for OT. (PM)

Figure X–33. Joint interoperability testing operational testing entrance criteria template

Appendix Y

Threat Considerations for Testing

Y–1. Overview of threat considerations in testing

Army policy requires that testing include an accurate representation of the threat projected to exist at a system post-IOC date. Threats must be identified, approved, and updated continuously throughout the system's life cycle (AR 381–11). Defense Intelligence Agency (DIA)-approved threat or system-specific threat definitions developed in accordance with appropriate regulations will be employed when tests are planned, designed, and conducted.

Y–2. Management of the threat during test planning

a. Testers are expected to understand the evolving threat and integrate it into tests that address COIC or exit criteria, AI, or technical characteristics and are realistic, representative, and credible. Threat-related issues should be managed using the following guidelines:

b. Coordination between testers and the system evaluator with the appropriate MACOM threat support organization (usually the TRADOC center or school threat manager) responsible for the production of the STAR and threat TSP should be established early and continue throughout test planning.

c. In addition to the approved COIC, the supporting threat organization must have access to the AI and the planning data embodied in the test design concept in the SEP. The test design includes the scope (that is, tactical scenarios, degree of operational realism, and types of test events), test factors and conditions (that is, control of factors to ensure test events occur under appropriate combinations of test conditions), and test design matrices (that is, grouping of test conditions into trials, vignettes, missions, and phases). Without this information, the TRADOC threat manager, who is drafting the threat TSP, will not be able to properly shape the threat to meet the objectives of the test. This will result in a threat TSP that is less than adequate to do the job and could result in the TISO (from DCS, G–2) pulling the threat validation from the test.

d. Since the threat TSP supports preparation of the EDP and DTP some of the interrelationships between the documents begins to emerge. The threat TSP must be prepared to meet regulation-specified test planning timelines. The supporting threat organization must receive test design data as early as possible. This all begins with the activities of the TCG.

Y–3. Threat coordination group

The system specific TCG should be stood up immediately after the formation of the T&E WIPT. (See para 5–14*b*.) It is the mission of the TCG to focus and refine the threat found in the STAR into the threat requirements for the tests. This can only be accomplished in a timely manner if the five key players (threat officer, TSM, evaluator, tester, and PM) coordinate early, continuously, provide the information requested, and have a clear understanding of the interrelationship that each has to the other for mission accomplishment. Once at least some of the threat requirements can be ascertained and locked by the TCG, then and only then is it time to stand up the TAWG. The TCG is also responsible for ensuring the adequacy of the threat resources as they are represented in the TEMP. If available, the most current threat VR will be used to assist in determining the adequacy of threat resources to represent the desired threat. Note that there is only one official report that looks at the overall adequacy of a threat—the VR. The Threat will continue to evolve and mature with time. That is why it is imperative that the TCG ensure the latest DIA validated threat assessments for all test specific threat requirements are reviewed and carefully considered for incorporation in all threat related documentation.

Y–4. Threat accreditation working group

After at least some of the threat requirements for the tests have been identified and locked by the TCG the TAWG is formed to accredit specific test application of threat simulators, targets, surrogates, and target arrays. The TAWG operates to approve these threat requirements and convert them into accredited threat resources for a specific test applications. When available, applicable threat system VRs are used to assist in determining the overall threat worthiness of threat test resources. Included in its membership are representatives from the same organizations that comprise the TCG as well as representatives of PM ITTS, threat simulator and target MATDEV offices, appropriate intelligence production center (IPC) analysts, and the MATDEV. The TAWG should meet at least 24 months prior to the test (T–720) in order to have adequate time to accomplish the following functions:

a. Ensure that the threat requirements identified and locked by the TCG are compared to the threat resources in the TEMP. Any changes must be clearly identified and documented.

b. Ensure that this new list of threat resources can be used to replicate the desired threat using actual threat articles, surrogates, simulators, or simulations. Where they cannot, this must be clearly documented as a test limitation and its impacts assessed and reported in the threat TSP or its accompanying Threat System Accreditation Report (TSAR).

c. For OT, ensure that threat resources documented in the final OTP reflect threat requirements identified by the TCG and that can be accredited by the TAWG are what is submitted to the TSARC for approval prior to the test. This will give a true reflection of the actual threat costs for the test, showing availability, accreditation potential, and requirement fulfillment.

d. Accredit the use of designated threat simulators/targets for each test.

e. Identify differences ("deltas") between the simulators or targets and current estimates of corresponding threat system characteristics and assess their impacts on the test.

f. Through comparison of the drafts of the threat TSP and the SEP, accreditation offers a timely opportunity to reconcile differences between them. Also, this facilitates development of test planning guidance as a basis to complete the SEP and provide increased assurance that the threat resources identified are sufficient to represent the threat with greater fidelity during the test.

Y–5. Threat in test readiness reviews

TRADOC is responsible for validating the planned threat portrayal. For tests including force-on-force trials, TRADOC also validates the threat force training plan prepared by the threat manager. For OT, this validation is documented in the OTRS prepared by the CBTDEV. The ATEC Threat Support Activity also participates to report of the preparedness of threat simulators.

Y–6. Deviations from the threat

When significant deviations from the validated threat are expected in test portrayals, whether due to a lack of threat resources or situations dictated by testing requirements, and/or it is determined that potential portrayal shortfalls pose significant risks to test validity, the appropriate threat manager and threat integration center should be consulted as soon as these are identified so they can seek offsets or alternatives to minimize potential threat-related test limitations. The TRADOC threat manager must be forthright and inform the testers and evaluators where deviations can and cannot be accommodated. The threat manager should immediately notify TRADOC Assistant Deputy Chief of Staff for Intelligence (ADCSINT) Threats, T&E Division for assistance. As required TRADOC should seek formal DCS, G–2 TISO recommendations for any alternative solutions that may have been missed to permit early resolution of problems. Once the threat TSP has been finalized and approved by DCS, G–2 and for OSD T&E oversight programs, reviewed and concurred with by DIA, deviations become much more problematic. Testers and evaluator must be able to clearly articulate to the threat intelligence community why these deviations are necessary and work with them to find an acceptable solution that will not result in the validity of the threat portrayal to be compromised.

Y–7. Threat portrayal fidelity

Due to resource limitations (availability of threat systems in the quantity, fidelity, and diversity sometimes required), it is unlikely that the threat force in a test will be represented with total fidelity to the threat as described in the STAR, especially in OT, nor is it really expected to. What is expected is that the threat requirements identified and locked in the TCG process, accredited in the TAWG process, and documented in the threat TSP and its accompanying TSAR that have been specifically designed for the test will be represented with total fidelity. This however, is not always the case. The degree to which threat force operations will be faithfully represented during the test will be based on subjective judgments of the TRADOC threat manager and the level of training of the threat system operators.

Y–8. Threat critiques

Intelligence personnel supporting or observing test preparations and/or execution should direct commentary or critiques on the threat portrayal through the evaluator. These critiques and commentary should be as specific as possible and include the significance of the comment or critique to the overall threat portrayal during that trial or vignette. It is the responsibility of both the Intelligence Representative and the Evaluator to come to an agreement as to the significance. This will ensure that only those comments deemed relevant to the interpretation and evaluation of test results are communicated to other personnel directly associated with the test.

Y–9. Resolution of threat shortfalls

Normally, the CBTDEV and MATDEV who are responsible for the STAR and threat TSP, assist in setting up the test and overseeing its threat-related aspects. The Army validating authority for threat portrayals, will be on-site and is

capable of interpreting the significance of threat-related issues on test validity, thereby minimizing the potential for controversy.

Y–10. Threat test limitations

Significant portrayal shortfalls must be included in test reports as "test limitations" and their impact on test validity assessed in T&E reports.

Y–11. Threat is dynamic and uncertain

The threat to be portrayed in testing results from an intelligence estimative analytical process that assesses specific military capabilities of a potential enemy usually at future point in time. Although uncertainty is inherent in all intelligence, estimative intelligence, due to the limited availability of collectable information, to a greater degree than other types of analytical disciplines, is heavily reliant on applied methodologies usually derived from the physical sciences. As new intelligence is developed and intelligence gaps narrow or close as a result of supplemental collection and analysis or evolving methodologies, the threat may change. If the DA TCG determines these changes to be substantial, they must be incorporated into T&E activities.

Y–12. Threat in test planning

The STAR is used to define the tactical context to support development of the TEMP, OTP, and the SEP.

Y–13. Threat test support package

The threat TSP is a document (or set of documents) that provides a description of the threat against which the new system will be tested. It is required for all materiel programs. Derived from the STAR, the threat TSP is more detailed and is used in developing the test environment necessary to prepare the final SEP and provides the threat scenarios for each operational test. Determination of the threat year and scenario selection for the test will be made by the T&E WIPT upon the recommendation of the MATDEV and the system evaluator. The development of the threat TSP (both initial and final) cannot be done in a vacuum. It takes close coordination between and amongst all the principal participants (threat manager, tester, evaluator, TSM) to ensure that nothing becomes disjointed. Each of the principal participants has an important function. Evaluator provides the initial drafts of the SEP, MOPs, MOEs, and Failure Definition Scoring Criteria. The tester provides the initial drafts of the test concept to include the terrain over which the test will be conducted. The TSM provides the overall capabilities and limitations of the system and the concerns of the CBTDEV. As each of these is refined and matured, they are provided to the threat manager and potential impacts, changes are discussed and agreed to. An initial threat TSP is developed immediately after MS A to support future testing for a specific system or concept.

a. The threat TSP defines the threat portion of a realistic operational test environment adequate to test the developmental system in the context of related COIC or exit criteria and AI.

b. Preparation and approval.

(1) To support DT requirements, the MATDEV or PM (that is, threat support organization) will expand and tailor the initial threat TSP for each test for which threat force operations are to be portrayed realistically. It is here that the STAR is critical. Since the STAR outlines all the known threats to the system undergoing test, it provides DT with unique insights to potential vulnerabilities that are not limited to the geopolitical realities of one threat country or region.

(2) For OT, the CBTDEV, normally the TRADOC proponent center or school threat manager, prepares the initial threat TSP for each IOT, 18 months (T–540) before the test start date. This date is not hard and firm. Rather, it is flexible based upon the needs of the system undergoing test; and the availability of information required to construct the document. The due dates for both the initial and final threat TSP should be coordinated and approved in one of the first meeting of the T&E WIPT. For other tests (FDT/E, EUT, LUT, or FOT), a threat TSP will be prepared unless the T&E WIPT acting upon the recommendation of the system evaluator, determines that a validated threat portrayal is not required for the test. The requirements of the COIC operational test design concept, and TEMP will form the basis for a recommendation to waive the threat TSP.

(3) For user testing of tactical systems, the threat integration center, usually the TRADOC ADCSINT Threats, T&E Division, approves/validates the threat TSP, from a tester's perspective, to ensure that threat operations are portrayed accurately and consistently. DCS, G–2 is the validation authority for threat TSPs for ACAT I, ACAT II, and ACAT III systems on the OSD T&E Oversight List and provides a copy to DIA for review and comment. Most threat TSP for OT of other Non-major systems are approved and validated by the TRADOC ADCSINT Threats, T&E Division, while this is done by appropriate AMC foreign intelligence officer, when a threat TSP is required to support DT. The final threat TSP to include all appendices is dependent upon the coordinated completion of the test trials and

vignettes (coordination between tester, evaluator, TSM, and threat manager) and the threat system accreditation report. The final threat TSP must be approved and validated 12 months before the test date (T–365), or as coordinated in the T&E WIPT for the system undergoing test.

c. The threat TSP format and content is detailed in AR 381–11. It is prepared in modular format to facilitate the updating process from test to test since only those parts required for a given test need to be completed. Section III (Threat) of the threat TSP often requires revision, since the AI and the SEP continue to evolve.

d. When approved, the threat TSP describes the threat to be used for planning and developing the test and to be portrayed during test execution. An approved threat TSP, however, does not ensure that test threat portrayal is valid. Two separate approval actions are required, one for the threat TSP and one for the threat portrayal during the test. The approved threat is included in the SEP prior to testing.

Y–14. Integration of threat data in operational test planning and threat and evaluation measures of effectiveness and measures of performance

Although the system evaluator has access to threat intelligence (for example, STAR) shortly after program initiation that is used to define the tactical context for the test, actual integration of the threat into OT does not begin until after completion of the functional dendritics, which do not consider the threat. The dendritics for each system are used to define system functions and subfunctions, clarify primary MOE derived from the COIC, and formulate MOP and data requirements necessary for OT. Even though the functional dendritics do not take into account the threat when they are used to formulate the MOP and MOE; the formulation of the MOP and MOE are essential in the identification of the Threat Requirements for a given test. MOP and MOE are used as limiting factors in determining both the threat that is required (system types and capabilities) and the threat that although a viable threat to the system undergoing test has no bearing upon the outcome of this particular test.

Y–15. Test factors and conditions for threat

Threat becomes operative as the system evaluator endeavors to identify factors (that is, test variables likely to effect test event outcomes) and the conditions (that is, discrete aspects of a factor, or factors, often expressed as a range of values, capabilities, or operational modes). Threat data (such as the types and echelon of forces, types and numbers of systems, and doctrine and tactics) which determine threat force movements and operations under varying situations, become factors and conditions for purposes of developing a test concept. Once these determinations are made, usually through use of a matrix approach keyed to each COIC, the system evaluator then must decide how each factor and condition, including those related to the threat, will be controlled during testing (that is, "fixed," "systematically varied," "tactically varied," or "uncontrolled").

Y–16. Threat and the tactical context

The STAR is used to define the tactical context describing the threat environment and threat systems that will exist at the IOC date and throughout the life cycle of the developmental system. The evaluator uses the STAR and information developed in the TCG process to identify the tactical setting as well as develop the factors and conditions to formulate the "test approach" section of the SEP. The system evaluator must make this same information available to the appropriate threat support office, usually the TRADOC center or school threat manager, as early as possible, in order to expedite preparation of the threat TSP, which is essential to development of the SEP. As the tester refines the test approach guidance developed by the evaluator, must continue coordination with the threat manager to ensure timely completion of a threat TSP tailored to test requirements.

Y–17. Threat and the operational test environment

The OT environment is the "Force-on-Force" application of the Defense Planning Guidance scenario in an OT (combat situation). Once the T&E WIPT, based upon the recommendations of TRADOC ADCSINT Threat, T&E Division, determines the most appropriate Defense Planning Guidance TRADOC standard scenario to be used in the test, the TCG core members (DIA and supporting IPC; DCS, G–2; and TRADOC ADCSINT Threats) craft the threat operational environment or combat situations in which the system will be tested at the post IOC time (usually IOC + 10 years). The combined effects of the combat situations in the force on force ("blue" vs. "red") create a unique opportunity to measure the combined and cumulative effects of both enhancing and diminishing factors on the test.

a. Enhancing factors. The "blue" organization, TTPs, and doctrine of employment are integrated so that operational effectiveness of the system is enhanced.

b. Diminishing factors. At the same time, a system's operational effectiveness is subjected to diminishing factors. The chief diminishing factor standing between the system and the achievement of its mission is the "red" organization,

TTPs, and doctrine of employment. Other factors include the effects of weather, terrain, and interference from other systems.

Y–18. Threat in the developmental test environment

Within DT, the tester and evaluator are free to run the gambit of all threats as outlined in the STAR without regard to country of origin or the impacts of any existing or projected political-military realities. This affords the tester and evaluator the ability to truly stress the system under test. This allows for the creation of a true worst case scenario and environment where the most lethal threats real and projected from a host of countries can be combined and there combined effects measured.

Y–19. Test profile

threat TSPs contain threat profiles, system profiles, and environmental profiles. Test designers merge threat, system, and environmental profiles into test profile sets that are incorporated into the SEP.

Y–20. Threat profiles

The threat TSP contains individual test threat profiles consistent with the overall test objectives, scenarios, and threat resources to be used. Threat profiles describe the types of threat and threat equipment that the system is likely to encounter, specific threat effects anticipated, threat tactics and countermeasures, threat doctrine and employment practices, and threat organizations. The operational tester uses the threat profiles to develop the OT environment and the target arrays for the test.

Y–21. Scoping of threat in test profiles

Because the number of possible test profile sets is so large and COIC can be resolved through analytical means other than OT, it is neither economical nor desirable to develop threat profiles for every possible profile set. Therefore, the tester must monitor the preparation of the threat TSP closely to ensure that threat profiles are—

a. Configured appropriately for the environmental conditions and means of employment (tactics, doctrine, and organization) that are most important in order to respond to the test issues.

b. Developed only for those aspects of a threat profile that are technically possible, operationally feasible, and realistic.

Y–22. Threat profile complexity

Because the threat TSP becomes progressively more complex during the system development process, test threat profiles also increase correspondingly in scope and complexity.

a. For EUT, the test threat profiles focus on potential targets, countermeasures, and opposing weapons at the single system one-on-one level.

b. For IOT&E, the test threat profiles, depending on the developmental system, can expand to include opposing forces up to the battalion level.

c. At follow-on OT&E, the test threat profiles include an updated configuration of potential opposing forces at all levels.

Y–23. Threat scenarios

a. Defense Planning Guidance. The annual Defense Planning Guidance, issued by the Secretary of Defense, provides a set of common planning assumptions for U.S. and friendly forces and planning scenarios projected for a 10-year period. It also defines strategy and force options identifying the specific operational environments in which U.S. forces must be prepared to function. The Defense Planning Guidance is also the basis for development of U.S. Army scenarios to support the force and materiel development processes.

b. U.S. Army Training and Doctrine Command standard scenarios. The purpose of a standard scenario is to provide consistency and reduce bias for all combat development programs through use of a common base case that portrays TRADOC-approved U.S. Army doctrinal and operational concepts. The TRADOC Analysis Command is the proponent for scenario development for friendly forces, while TRADOC ADCSINT Threats, T&E Division, assists in preparation of the threat force scenario, which is validated by DCS, G–2. TRADOC standard scenarios are considered in the development of threat force scenarios in the threat TSP and preparation of the Integrated Threat Tactical Operations Plan, both of which support the test design process. During OTP preparation/preliminary test design planning, the system proponent and the operational tester, based upon recommendations from TRADOC ADCSINT Threats, T&E Division and subject to T&E WIPT approval, select the standard scenario for use in testing. Both friendly and threat test operations must be compatible with the selected standard scenario. It is this Defense Planning

Guidance based scenario that serves as the backdrop for the test. With the test trials and vignettes (snapshots in time out of the chosen Defense Planning Guidance based TRADOC scenario) being carefully selected for their operational context and their ability to properly frame each portion of the test.

c. Integrated threat tactical operations plan. The integrated threat tactical operations plan is an instructional guide for the operation of simulators also useful in test planning, specifically as a reference in preparing both the SEP and the DTP. It is produced by the ATEC Threat Support Activity, approved by ATEC, and validated by HQDA.

Y–24. Threat depiction in environmental profiles

These profiles define the terrain, weather, communications, and transportation infrastructures, friendly interference (for example, RF), time and distance separating operating forces from their support structure, and other nonthreat conditions under which the test is to be conducted. The test environmental profiles are drawn from the system requirements documents and supporting analyses.

Y–25. Threat adequacy

a. The COIC may require measurement of the combined impact of the factors that enhance and diminish operational effectiveness on lethality and survivability or the multiplying effect of one system on the lethality and survivability of another system. When either circumstance exists, the operational tester and system evaluator with the assistance of the TRADOC ADCSINT Threats, T&E Division must ensure that the threat portrayed in the test will be sufficient to support the system evaluation of direct effect systems as well as the impacts of indirect effect systems.

b. Lacking an adequate threat portrayal that considers both types of systems, the evaluator will be unable to make accurate assessments of system operational effectiveness.

Y–26. Threat and modeling and simulation

Threat considerations in employing M&S may be based on the following—

a. Threat-related resource limitations. Estimated threat capabilities cannot be adequately represented due to a lack of threat simulators, targets, or threat surrogates that match estimated threat capabilities.

b. Uncertainties and variables. M&S techniques have considerable potential for improving the fidelity of the portrayal of threat in OT activities. There are significant uncertainties related to the estimates of future threat capabilities that should be carefully considered in all OT activities. Sensitivity analyses, using M&S techniques, can be applied to examine the impacts of incomplete or uncertain estimative intelligence on testing. In addition, M&S can assist in projecting the implications of future enemy reactive threat to the system being tested. Typical aspects of the threat that lend themselves to M&S techniques include—

(1) System performance characteristics, for which IPCs develop their best estimates that normally become the basis for OT design, as well as high and low parametric values as a means of "bounding" the uncertainties.

(2) Variables related to evolving threat forces as a result of materiel upgrades, organizational changes, and modifications of doctrine and TTP.

(3) Scenario-related operational options involving the types of combat operations being portrayed (for example, main attack versus supporting attacks, or offense versus defense).

c. Pretest modeling and simulation applications.

(1) An important use of M&S techniques in test planning is the refinement of test scenarios and data matrices to decide which elements of system performance should be the focus of OT. To do this, the M&S used must relate the operational effectiveness and suitability of the system in a realistic scenario, with appropriate force levels using situations identified in the OMS/MP. This allows the system evaluator to do sensitivity, contingency, and functional analyses for various technical and force mix assumptions.

(2) There is a perceived need in designing tests to compare (or determine the differences or deltas) between the performance of threat simulators and targets deployed in the test array and evolving intelligence estimates of the characteristics and capabilities of the actual threat systems.

Y–27. Threat support to model-test-model concept

Although there are rigorous VV&A procedures for the application of M&S techniques in OT, an essential prerequisite for their use is a process to ensure that threat representations and usage modeled or simulated are consistent with approved estimative intelligence through Army and DIA validation.

a. Approval or validation of threat data. The threat represented in the model must be documented and traceable to an approved and validated STAR and threat TSP, or to automated threat data from other approved Army high- and low-resolution models. The threat portions of M&S developed by TRADOC are approved by TRADOC ADCSINT Threats, T&E Division and validated by DCS, G–2. Threat data to be used in M&S applications, however, are

validated by TRADOC ADCSINT Threats, T&E Division. Deviations from threat data contained in DCS, G–2 and DIA approved intelligence, however, must be fully documented and approved by DCS, G–2 before use.

b. Threat requirements for sensitivity analyses. If M&S is appropriate to conduct sensitivity analyses related to uncertainties in the threat, the system evaluator will require a range of threat alternatives or variables (that is, threat force weapons and systems parameters and/or doctrinal, organizational, or operational options derived by intelligence analysts).

Y–28. Accreditation of threat input to modeling and simulation used in test and evaluation

Just as Threat Simulators and Targets must be accredited to determine their appropriateness and suitability for use in OT, so must any and all threat data within a model or simulation be accredited for its appropriateness and suitability for use in a given OT event. This includes, but is not limited to Ph and Pk tables, doctrinal templates, threat system characteristics and performance tables, TTPs, and so forth. TAWGs for M&S must be convened as soon as the T&E WIPT or one of its subordinate IPTs identifies M&S applications to be used in the test.

Y–29. Intelligence production centers

IPCs, such as the National Ground Intelligence Center and the Missile and Space Intelligence Center perform a critical role in providing the T&E community with a realistic threat environment. IPCs (that is, depending on the threat to be portrayed, National Ground Intelligence Center or Missile and Space Intelligence Center) provides the following assistance:

a. Produces and disseminates general military and scientific and technical intelligence used by test planners and evaluators to determine system effectiveness and suitability.

b. Produces intelligence to satisfy regulatory responsibilities that Army systems be tested in a realistic threat environment.

c. Participates in Validation Working Groups and TAWGs to ensure proper threat data are being utilized in the design, development, and fielding of targets and threat simulators/simulations.

d. Participates in TCGs and T&E threat working-level IPTs to assist in the integration of the appropriate threat data in test planning and design.

Appendix Z

Instrumentation, Targets, and Threat Simulators

Section I

Planning and Use

Z–1. Overview

a. Instrumentation, targets, and threat simulators planning and use. This appendix provides general planning guidance for ITTS in support of T&E requirements. It outlines the relationships of key activities involved in planning, managing, and using ITTS in support of T&E and describes procedures for scheduling and use. The term "ITTS" as used in this appendix includes simulations. Section II prescribes procedures to be followed in the validation and accreditation of threat simulators/simulations and targets. Section III outlines the responsibilities for those organizations associated with the planning, use, and participation in the procedures prescribed by this appendix.

(1) Threat representation and major instrumentation programs are considered Army ACAT III programs. These programs yield complex hardware and/or sophisticated simulation products. They are consequently governed by the same acquisition rules that apply to most Army developments, and are assigned to the PM ITTS for programming and execution. Threat representation programs have their own peculiar acquisition planning considerations, but the key to successfully planning and integrating threat representations into testing is the early involvement of PM ITTS, ATEC, the system PM and the Intelligence Community through the T&E Working Integrated Product Team (T&E WIPT).

(2) This appendix describes the planning and use for "common use" and "system specific" threat representations. Common use threat representations are those developed or acquired in support of more than one blue weapon system, whereas system specific threat representations are developed or acquired for only one. PM ITTS funds for common use threat representations by programming their requirements through the Test Budget Operating System manager, the TEMA. System specific threat representations are funded by the blue weapon system PM through the Equipping Program Evaluation Group.

(3) Planning for instrumentation and threat representations must occur early in the blue system development process in order to be available for use in support of specific T&E events. Preliminary determinations and related funding estimates must be incorporated both in the TEMP and in the SEP. This means that test resource planning must be substantially complete prior to project management office development of a cost analysis requirements document. This also requires that detailed planning be completed prior to ATEC's submission of OTPs to the TSARC. Early planning for threat representations and instrumentation is thus key to the successful and timely execution of a testing program.

b. Definition of terms used in this appendix.

(1) *Test instrumentation.* Test instrumentation is a generic term that includes all instrumentation used by testers, to include—

(a) Scientific or technical equipment used to measure, sense, record, transmit, process, or display data during test or examination of materiel.

(b) Simulators, system stimulators, or threat instrumentation used to measure or depict the threat for training, teaching, or proficiency during testing.

(c) Targets used to simulate a battlefield object when destruction of the real object is not practical or the actual object is not available.

(2) *Threat representations.* Threat representations include models, simulations, simulators, emulators, foreign materiel (that is, actual systems), and aerial and ground targets that portray specific foreign military weapon systems or civilian devices used in an adversarial military role. Threat representations are generally grouped in two specific categories—

(a) Threat systems. A threat system is a generic term used to describe simulators, emulators, foreign equipment instrumented for T&E, a model, a simulation federation representing foreign military equipment, or multiple integrated federations. Threat systems portray potential adversary systems and their operation in tactical environments. Simulators and emulators have one or more characteristics that, when detected by human senses or manmade sensors, provide the appearance of an actual foreign system with a prescribed degree of fidelity. When embedded in simulation, validated threat systems portray foreign equipment, its operation, and its tactical employment with high fidelity. This includes signature, communications, performance, lethality, and a host of other factors. Threat systems are generally re-used many times. They are not normally expendable.

(b) Targets. There are three classes of targets. They are ground, aerial, and virtual. Targets are normally economical, expendable devices used for tracking and/or engagement by missiles/munitions in support of T&E. This factor

normally differentiates targets from threat systems. However, targets have other uses. They can, for instance, be utilized multiple times for hyper-spectral data collection in support of research, development, and acquisition. Targets may be mobile drones controlled by programs or by real-time link. Some targets are not mobile. Ground targets are intended to represent an adversary ground vehicle system or ground based military structure. Aerial targets are intended to represent adversary aircraft or cruise or tactical ballistic missiles. Targets may represent only selected adversary system characteristics or they may faithfully represent all aspects of that equipment. Targets may, in fact, be actual pieces of foreign military equipment not useable or instrumented as a Threat System. Virtual targets provide validated, digitized spectral images of specific foreign military hardware. Digitized structural information representing some foreign military equipment may also be available as virtual target data.

(3) *Major instrumentation, targets, or threat simulators or simulations.* Projects are designated major based on a variety of factors, such as acquisition complexity, assessed relative technical risk, schedule risk, cost, and applicability to other mission areas or services. A project classification decision tree, as well as additional discussion of the design, development, and procurement of such items is discussed in paragraph Z–3.

Z–2. Planning for instrumentation, targets, and threat simulators

a. Planning for specific ITTS to support T&E must begin early in the weapon system Concept and Technology Development phase to ensure timely and adequate support. Requirements identification and documentation for targets and threat simulators/simulations is described in paragraph Z–6, and major instrumentation requirements identification is described in paragraph Z–7. Long-range planning for ITTS follows the process described in paragraph Z–8 of this appendix.

b. When planning for the use of targets and threat simulators, it is important to know how threat information for a United States system is derived and where the information is documented. While these documents are primarily intended to support and justify the development of materiel systems, they are also useful in planning for target and threat simulator/simulation support for the T&E of the system. Such documents include ORD, integrated program summary, cost and operational effectiveness analysis, AoA, TEMP, SEP, outline test plan, threat TSP, STAR, integrated threat tactical operations plan, and baseline intelligence products.

c. ITTS acquisition is accomplished through a tailored DoD 5000 series acquisition process by the PM ITTS. PM ITTS is the Army's single manager for developing and acquiring targets (except training range targets), threat simulators/simulations, and major instrumentation in support of testing. All test activities, PMs, and other MATDEVs will coordinate their ITTS requirements with PM ITTS beginning with concept and technology development and continue through the life cycle of the system. It is PM ITTS' responsibility to plan, program, fund, and execute all non-system unique ITTS requirements. It is the responsibility of the PM plan, program, fund and execute all system unique ITTS requirements. Only in those unique cases where PM ITTS cannot provide the ITTS support will the system PM pursue alternate ITTS execution.

Z–3. Needs satisfaction

Major instrumentation, targets, and threat simulator needs will normally be satisfied from on-hand assets. Satisfaction of needs in excess of on-hand assets should make use of one or more of the following methods, listed in order of preference under major instrumentation and threat representations:

a. Major instrumentation.

(1) Testers are encouraged to survey and query existing inventory databases at ATEC and PM ITTS to determine what resources are available, where they exist, and in what quantities. Direct coordination with designated points of contact is necessary to ensure availability of their latest data and to gain a complete understanding of an item's capabilities, limitations, support requirements, and suitability, as well as to determine its potential availability. The preferred alternative for meeting instrumentation and test support equipment shortfalls should be through the interrange loan agreements process. The Range Commander's Council operates a Tri-Service forum for sharing of test support equipment and instrumentation. Refer to the Range Commander's Council Secretariat, ATTN: STEWS–RCC, U.S. Army White Sands Missile Range, NM 88002–8110.

(2) Standard off-the-shelf instrumentation may be leased or rented to satisfy short-term inventory augmentation or one-time needs. A cost benefit analysis should be conducted to compare total lease or rental costs to NDI life cycle (procurement plus ownership) costs over the full instrumentation requirement period before this option is pursued.

(3) Testers may procure standard off-the-shelf NDI instrumentation or modify on-hand inventory assets needed to satisfy test requirements. A trade-off analysis of modification versus procurement of NDI (assuming availability) should be conducted to determine the most cost efficient approach.

(4) Design, development, and procurement of instrumentation should be the exception due to the time and expense associated with such an effort. Experience has shown that the acquisition cycle for non-major instrumentation can

easily take 3–5 years and 8–12 years is not uncommon for a major instrumentation system. When development is necessitated, the impact must be closely coordinated through the T&E WIPT and the TSARC, documented, and reflected in the TEMP as a potential test limitation. Figure Z–1 provides an instrumentation project classification decision tree. It should be used as a guideline for determination of major versus non-major ITTS.

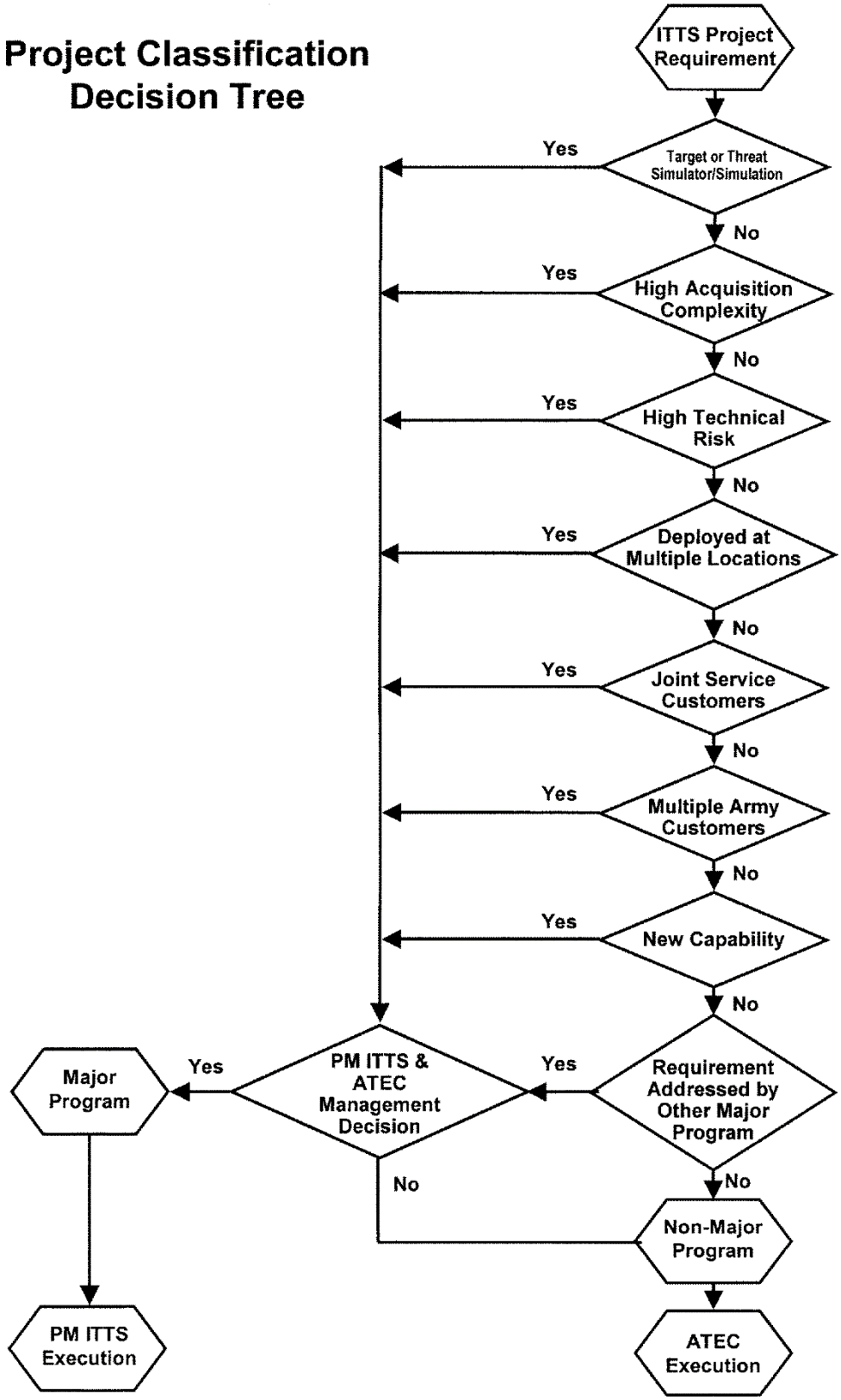


Figure Z–1. Project classification decision tree

b. Threat representations.

(1) Testers are encouraged to query existing inventory databases at PM ITTS as well as other sources such as the Defense Modeling and Simulation Resource Repository (https://www.dau.edu/tools/air-force-modeling-and-simulation-resource-repository-msrr) and the Defense Intelligence Modeling and Simulation Resource Repository to determine what resources are available, where they exist, and in what quantities. Direct coordination with designated points of contact is necessary to ensure availability of their latest data and to gain a complete understanding of an item's capabilities, limitations, support requirements, and suitability, as well as to determine its potential availability. The point of contact for Threat Systems is PM ITTS Threat Systems Management Office (TSMO), Refer to: Director, Threat Systems Management Office, AMSTI–ITTS–S (Operations Team Lead), Bldg 4497, Redstone Arsenal, AL 35898–7461, Telephone (256) 876–9656. The point of contact for Targets is the PM–ITTS Targets Management Office, AMSTI–ITTS–Q, Redstone Arsenal AL 35898–5798.

(2) Design, development, and procurement of threat representations should be the exception due to the time and expense associated with such an effort. When development is necessitated, the impact must be closely coordinated through the T&E WIPT and the TSARC, documented, and reflected in the TEMP as a potential test limitation. Requirements for developments will be referred to the threat systems IPT for prioritization and potential funding.

Z–4. Schedule and use requirements

a. Individual test activities, directorates, ranges, and laboratories possess organic instrumentation assets consistent with their mission focus. Scheduling of organic instrumentation assets is affected in consonance with internal operating procedures. Scheduling of instrumentation assets from external sources is affected by direct coordination between the borrower and lender. Costs associated with instrumentation use are normally limited to those of lease, round trip transportation (if borrowed), and any modifications required for unique or special applications or interface requirements. The latter are typically charged to the customer (that is, the PEO or PM). Costs should be reflected in the OTP for TSARC approved tests.

b. For TSARC approved tests, requirements for targets will be included within the OTP. Targets developed by PM ITTS are subject to the provisions of validation and accreditation outlined in section II of this appendix. Individual test activities possess limited organic target assets. The vast majority of aerial and ground targets used in support of Army T&E are developed, procured, maintained and operated by the Targets Management Office. Specific procedural requirements for assets held by other organizations should be coordinated directly with their appropriate point of contact. Requests for use of assets controlled by the Targets Management Office will be documented on SMI Form 1209. Refer to Project Manager for Instrumentation, Targets, and Threat Simulators, ATTN: AMCPM–ITTS–Q, Redstone Arsenal, AL 35898–5798.

c. For TSARC approved tests, requirements for threat simulators/simulations will be coordinated with TSMO and included within the OTP. Specific procedural requirements for assets held by other organizations should be coordinated directly with their appropriate point of contact. Scheduling of TSMO assets is accomplished through direct coordination with them and should be affected no later than 24 months in advance of the required test date. Formal schedule coordination and approval for use is conducted as a part of the TSARC process. For all types of test and training support, TSMO will prepare a cost estimate for use in communication and coordination with the customer. For TSARC approved tests, costs associated with threat simulator support will be included within the OTP.

Z–5. Associated data for planning and use of instrumentation, targets, and threat simulators

In addition to the system documentation and reports mentioned in the preceding paragraphs, additional databases and inventories are available for reference when planning and scheduling the use of instrumentation, targets, and threat simulators. Some of these include the following:

a. Test facilities. ATEC Headquarters Instrumentation Division manages a database as a tool to identify existing Army major test facilities, major instrumentation, and test equipment. The database identifies assets by location, value, capability, and points of contacts to provide the test community with a readily available list of assets. Narrative descriptions and performance information identify system-unique capabilities of the facilities listed, while a list of major projects and programs supported enables identification of any similar or related uses that have already employed the facility. Refer to Commander, U.S. Army Test and Evaluation Command, CSTE–OP–IN, 4501 Ford Ave., Alexandria, VA 22302–1458.

b. Automated Joint Threat Systems Handbook. The Automated Joint Threat Systems Handbook is a stand-alone information retrieval database used for mission planning of joint and single Service exercises and preliminary planning of test projects. It provides user information on threat representative simulators, targets, actuals, models and simulations and related test ranges. Users are able to search for one or more test and/or training assets, associated technical

data, and points of contact for additional information and scheduling. It is available on CD–ROM for stand alone operation and can also be accessed via SIPRNET. For additional information, contact the Threat Systems Office, DOT&E.

c. U.S. Army Test and Evaluation Command Instrumentation Development and Acquisition Program. The ATEC Instrumentation Development and Acquisition Program is an automated instrumentation requirements database that incorporates instrumentation requirements for ATEC and its subordinate commands. The database is used to outline current and long range instrumentation requirements, funding and schedule requirements, and life cycle planning. Refer to Commander, U.S. Army Test and Evaluation Command, CSTE–OP–IN, 4501 Ford Ave., Alexandria, VA 22302–1458.

d. Facilities and Capability Information for Test and Training. Facilities and Capability Information for Test and Training (FACITT) is a Web-based information search tool created to satisfy the DoD requirement for locating both DoD and non-DoD facilities and capabilities that could perform test and training activities. Leveraging off the existing websites at these facilities, FACITT locates the facility and capability information through a focused Web-crawl and cataloging process. FACITT also includes linkable maps and catalogs that permit the user to link directly to the related sites. FACITT can be accessed at https://www.jcs.mil/.

e. Targets Information Manual. This manual serves as a descriptive catalog of Army targets and foreign ground assets available or in development for support of T&E or training. Refer to Project Manager for Instrumentation, Targets, and Threat Simulators, ATTN: AMCPM–ITTS–Q, Redstone Arsenal, AL 35898–5798.

f. Threat Systems Management Office Threat Inventory Database. PM–ITTS/TSMO maintains a database of all available assets for both hardware simulators and software simulation systems. These assets are available for use in testing and training. Refer to Project Manager for Instrumentation, Targets, and Threat Simulators at Director, Threat Systems Management Office, AMSTI–ITTS–S (Operations Team Lead), Bldg 4497, Redstone Arsenal, AL 35898–7461, Telephone (256) 876–9656.

Z–6. Threat requirements generation process for targets and threat simulators

This paragraph describes and figure Z–2 illustrates, in general terms, the process of identifying, coordinating, and prioritizing threat requirements in support of T&E. The objective of the process is to identify and prioritize those threats that must be replicated in the form of a target, threat simulator, or threat simulation in order to support T&E. The product of the process is a coordinated and prioritized list of requirements that can be considered for funding through the planning, programming, budgeting, and execution system process.

a. The process is initiated with the conduct of mission area analyses. Mission area analyses are conducted at each IPC, where science and technical intelligence is melded with general military intelligence to identify general threat trends and developments.

b. The next step in the process is primarily an intelligence-initiated series of threat conferences (see AR 381–11) to address more specific threats as they pertain to functional areas. Participants in this portion of the process include representatives from one or more IPCs, the DIA, appropriate PMs, the TRADOC, PM ITTS, and testers. The product of these conferences is a series of validated threat descriptions that U.S. Army weapon systems may encounter on the battlefield. Test specific threat items, however, are not identified during these conferences. The products of these conferences feed the STAR development process and are made available to the Research Development & Engineering Centers for the establishment of Science and Technology Objectives.

c. Another user of the threat conferences' product is the T&E WIPT. The T&E WIPT acts as a filter to refine the output from the conferences into test specific threats that will support the data collection requirements of individual tests. It is the responsibility of the T&E WIPT with guidance from the Threat Intelligence Community, to define the threats to be represented, the level of fidelity of the representations, and the environments in which the threat representations will need to operate (such as. open-air range, simulation, or within a specific architecture). This product of the T&E WIPT is input to the Threat System IPT requirements prioritization process and forms the basis of a "contract" between the tester and the PM as to the threats that will be used in testing. The T&E WIPT integrates these threat representations into an appropriate integrated testing strategy that is reflected in the SEP and the TEMP. The TSMO representatives to the T&E WIPT identifies existing threat resources that could be applied to the program and highlights shortfalls in threat resources. Shortfalls that are applicable to more than one development are reported to the Threat System IPT for budgeting and execution planning. Substantive threat issues that cannot be resolved by the T&E WIPT will be elevated through channels to the appropriate Threat Coordinating Group for resolution. If resolution is not achieved, the issues will be elevated to the program's Overarching IPT.

d. Following the filtering process by the T&E WIPT, the Threat System IPT prioritizes the threat requirements. This prioritization is reflected in the Army Threat Systems Master Plan (ATSMP), a document reflecting coordinated and prioritized threat requirements necessary to support the testing, training, and PM communities. The ATSMP is

prioritized jointly by ATEC and PM–ITTS and provided to TEMA for budgeting and programming consideration at HQDA. In the same manner, the ATSMP will also document system specific threat requirements in support of testing for individual PMs identified through the T&E WIPT for Army visibility and planning.

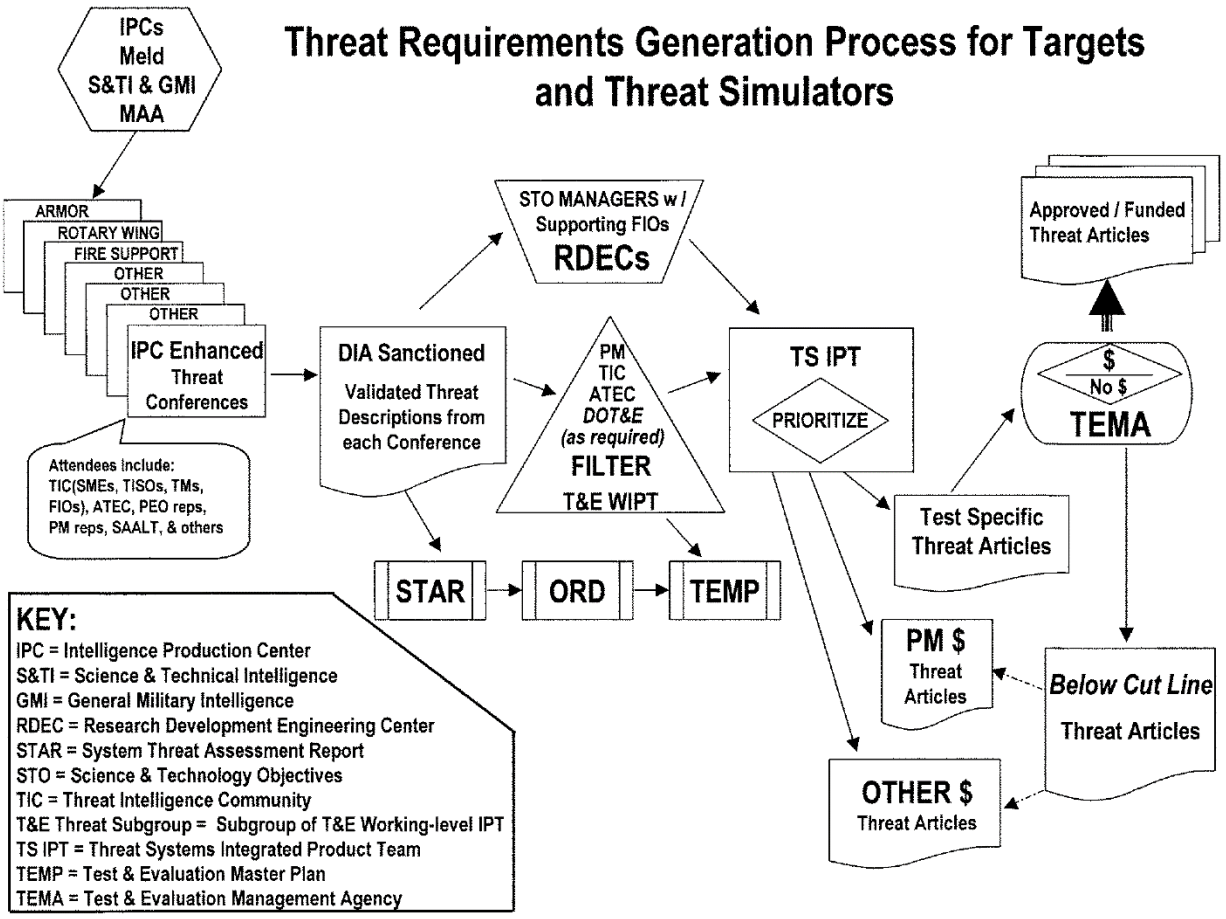


Figure Z–2. Threat requirements generation process for targets and threat simulators

Z–7. Major instrumentation requirements generation process

The process discussed in this paragraph provides general information for the user who is unable to fulfill instrumentation needs from inventory.

a. Each step of the major instrumentation requirements process is accompanied by the documents, actions and approvals required from the identification of a need by a user to the initiation of a project. The process and documentation requirements should be tailored based on agreement between the user and MATDEV. For all major instrumentation, the following are required:

(1) Formation of an instrumentation working group (IWG).

(2) Approval of documented requirements by a designated officer or civilian representing the user.

(3) Acceptance of the documented requirements by a designated officer or civilian representing, PM ITTS, the MATDEV.

(4) A joint agreement signed by both the user and PM ITTS that outlines the developer's approach, schedule and cost estimate.

b. The user (such as ATEC, a materiel development command, PEO, or PM) generates a requirement based on a need that is validated through documented references. These references may be the Army Science and Technology Master Plan, the FYTP, T&E WIPT minutes, the system TEMP, the Army Test Resources Master Plan (ATRMP) or any other such official document. The long range planning process described below provides the methodology used for identifying and refining requirements in the Army Science and Technology Master Plan. ATEC and the SMDC

will also identify needs to enhance their respective test facility infrastructure, improve testing efficiency, and improve operational safety. These needs will be documented by each command.

c. The user then reviews all requirements, checks for unwarranted duplication, and confirms adherence to the command long-range plan and the ATRMP. The user then performs the following functions—

(1) Prioritization of requirements.

(2) In conjunction with PM ITTS, identifies major instrumentation projects for management and execution in accordance with figure Z–1. Procedures specific to the interaction between ATEC, SMDC, and PM ITTS can be found in paragraph Z–13. Development programs not managed by PM ITTS will be internally managed by the user and are not addressed in this appendix.

d. For major instrumentation, PM ITTS and the user will form and jointly chair an IWG. The IWG will operate during the preparation and staffing of the documented requirements. The functions will be to mutually understand the requirements and establish general project milestones and documentation requirements.

e. The ITTS user will lead in preparing the documented requirements. PM ITTS and the U.S. Army Program Executive Office for Simulation, Training and Instrumentation (PEO STRI) will provide support as determined by the IWG. All documented requirements will be staffed within the using command and PM ITTS. The using commander (or designee), the test agency, PEO, or weapon system PM will approve and sign the documented requirements. A designated officer/civilian from PEO STRI will also sign the document as the MATDEV indicating the acceptance of the project and understanding of the requirement. The requirement documentation will be forwarded to TEMA.

f. The IWG will coordinate activities during the Concept Exploration phase. PM ITTS will study tradeoffs and prepare acquisition documents as required by the IWG. Trade-off studies may be performed as directed by the IWG. The user should select the best technical approach based upon projected resources and technical requirements. Both the user and PM ITTS will agree upon a development approach, schedule and cost estimate to satisfy the requirement. This agreement will be documented and jointly signed by the using commander (or designee), test agency, PEO, and a PM ITTS designee. The agreement will be forwarded to TEMA.

g. Joint Service reviews are required in the following instances:

(1) Projects competing for OSD T&E funds, are reviewed by tri-Service Reliance panels, comprised of subject matter experts organized by test capability areas. The results of these reviews are forwarded through the T&E Executive Agent structure for funding consideration as part of the Central Test and Evaluation Investment Program.

(2) Central Test and Evaluation Investment Program projects that are for short-term OT&E requirements only, are reviewed by the Office of the Secretary of Defense Test Investment Coordinating Committee (OTICC). The OTICC reviews all Services' OT&E requirements for unwarranted duplication and recommends a joint Service prioritized list of needs and solutions to OSD for funding consideration. As a result, potential OSD funded candidates and multi-Service duplications are identified.

Z–8. Long-range planning for instrumentation, targets, and threat simulators

TEMA will survey on an annual basis the technology capabilities of Army T&E facilities. The purpose of the survey will be to ascertain where future improvement and modernization investments should be made. The information resulting from the survey will be used to provide Army POM guidance and will be published as part of the annual ATRMP. The concept of the survey is evolving. The first survey was completed in the Fall of 2001 and published as part of the 2002 ATRMP, providing guidance for the FY 04–09 POM build. The first survey was conducted by gathering subject matter experts from test technology areas resulting in a series of roadmaps depicting required investments needed to maintain pace with emerging technologies and weapon systems development. Future surveys may follow a similar format or evolve into a different structure. Regardless of format, the objective will be the same; to roadmap the major improvement and modernization investments needed for T&E. In preparation for the annual survey, all commands involved with T&E should continuously review and update the T&E technology roadmaps published in the ATRMP.

Section II

Validation and Accreditation Procedures for Threat Simulators and Targets

Z–9. Overview of validation and accreditation procedures

a. This section provides the procedures used by the Army Validation and Accreditation Program for Threat Simulators and Targets. The processes, concepts, and procedures employed in validation and accreditation of targets and threat simulators are defined and prescribed. The roles and responsibilities of the DA agencies and organizations involved in validation and accreditation are identified in paragraphs Z–14 and Z–15 respectively. These procedures

implement and support DoD Threat Simulator Program Guidelines, chapter 3 of the Defense Acquisition Guidebook, concerning threat simulators/simulations and targets, and are issued in compliance with AR 73–1, DA Pam 73–1, and AR 381–11. Threat simulation, validation, and accreditation procedures can be found in AR 5–11 and DA Pam 5–11. Additional software-specific validation guidelines for submitting threat simulation VRs for use in support of T&E are currently undergoing development and will be published as interim policy guidance until the next publication of this pamphlet.

b. These procedures are applicable to Army threat simulators/simulations and targets, which represent a part or function of a specific threat system, and will be used in tests supporting milestone decisions. Exceptions to the validation process will be addressed on an individual basis. All requests for exceptions should be forwarded to the Director, U.S. Army Test and Evaluation Management Agency, 200 Army Pentagon (ATTN: DACS–TE), Washington, DC 20310–0200. A validation waiver, used to facilitate accreditation, does not preclude system validation requirements. Accreditation waivers are not granted.

c. Figure Z–3 illustrates the generic relationship of validation and accreditation support to the life cycles of Army materiel development and threat simulators/simulations and targets. As shown in the figure Z–4, validation is performed at critical points throughout the life cycle of threat simulators/simulations and targets. Accreditation pertains to specific test applications of threat simulators and targets during the operational phase of their life cycle. VWGs accomplish validations through a series of periodic meetings. The effectiveness of each VWG is entirely dependent on the ability of its membership to address a validation event for a given target, simulation or simulator. Validation must not be viewed as an evaluation where the relative worth of a system is being graded; it is a process for comparing simulators/simulations and targets to DIA-approved threat data, documenting the variations, and assessing the impact of those differences on the potential use of the simulator, simulation or target. The VWG task is finished: when the VWG members sign the completed VR; the report is forwarded to and approved by the Director, TEMA and, as required, forwarded to and approved by the DOT&E.

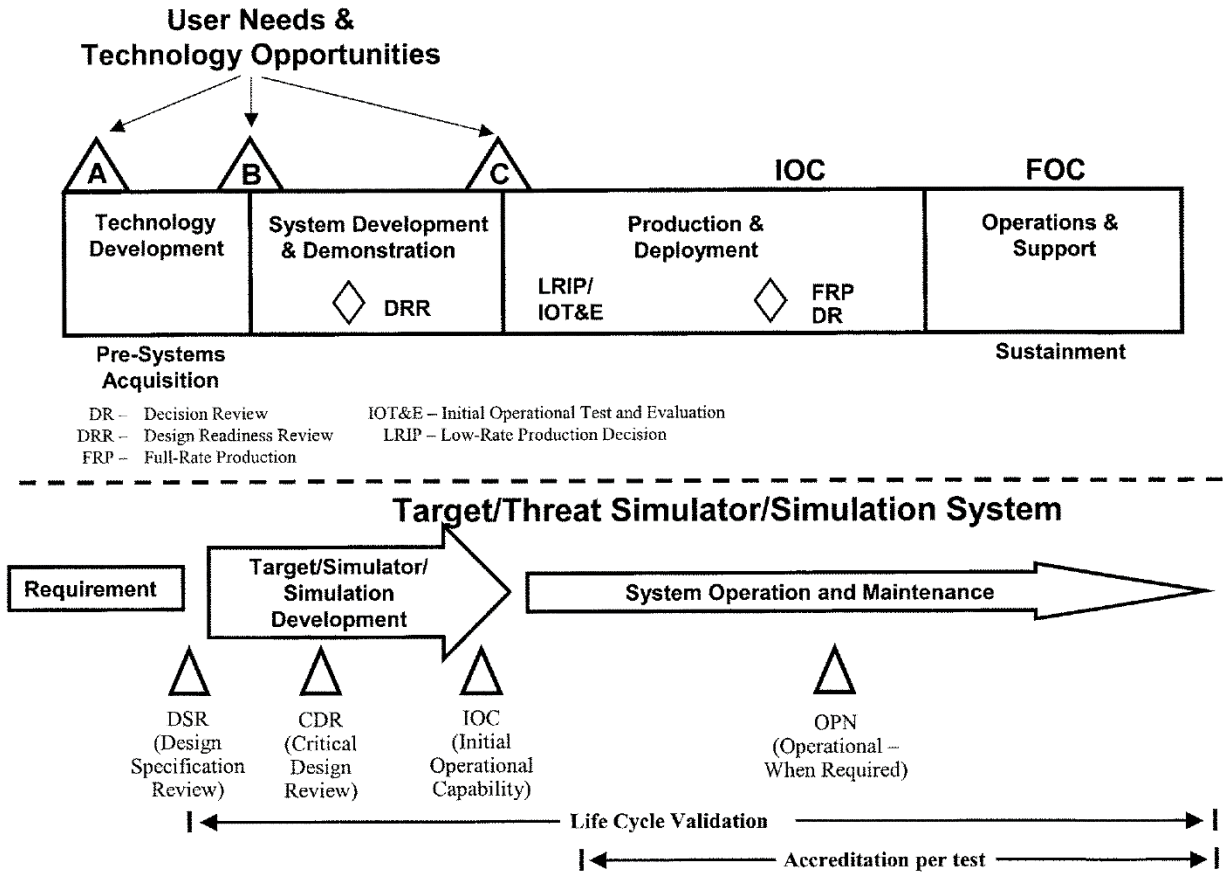


Figure Z–3. Validation/accreditation support to the Department of Defense life cycle model

Z–10. Validation of threat simulators/simulations

a. Validation is the process used to document and analyze critical performance differences a threat simulator/simulation may demonstrate when compared with DIA-approved data. Threat simulators/simulations are developed to portray actual threat system visual likeness and performance capability for user-identified test and training requirements. Accordingly, threat simulators/simulations may only duplicate or represent a limited number of threat system attributes. Therefore, threat system validation must be based upon expert knowledge of the threat, the simulator/simulation, and user requirements. A VR will be issued documenting specifics of the validation effort. Due to the differences in the validation of hardware (simulators) and software (simulations), the content of the respective VR will differ slightly as provided in the VR content instructions in table Z–1. Responsibility for funding developmental validation costs belongs to the threat simulator or target MATDEV. Periodic operational validation costs will be funded by the owning organization.

Table Z–1
Validation report format and content

Threat simulator/target validation report format	Threat simulation validation report format
Table of Contents	**Table of Contents**
EXECUTIVE SUMMARY This section is the last section written and is a condensed version of sections I through VI. The major elements of the six sections should be covered. No material is provided here that is not provided in the other six sections in greater detail. Much of the detailed discussion is not included here but is found only in the main body of the report. This section should be two to three	**EXECUTIVE SUMMARY** This section is the last section written and is a condensed version of sections I through VI. The major elements of the six sections should be covered. No material is provided here that is not provided in the other six sections in greater detail. Much of the detailed discussion is not included here but is found only in the main body of the report. This section should be two to three

Table Z–1
Validation report format and content—Continued

pages in length, unless there are a large number of differences and impacts to address. This should be a standalone section.	pages in length, unless there are a large number of differences and impacts to address. This should be a standalone section.
SECTION I INTRODUCTION 1. Purpose 2. Threat Representation 3. Points of Contact This section should briefly state what threat this simulator/target is expected to represent, what portion of the threat is included, what is left out, and the relationship of this simulator/target to others if it is a portion of a larger system, or a modification of a larger system. It also should state whether the simulator/target is expected to represent multiple variants of the threat, if such variants exist. The purpose or objective of the VR should be stated. This section should also include a statement that the VR describes the status of the simulator/target's ability to emulate the threat at that point in time, and that there may have been changes in the threat definition or in the simulator/target since the VR was written. The introduction should identify a point of contact for users to gain additional information.	**SECTION I INTRODUCTION** 1. Purpose 2. Threat Representation 3. Points of Contact This section should briefly state what threat this simulation is expected to represent, what portion of the threat is included, what is left out, and the relationship of this simulation to others if it is a portion of a larger simulation or a modification of a larger simulation. It also should state whether the simulation is represents multiple variants of the threat, if such variants exist. The purpose or objective of the VR should be stated. This section should also include a statement that the VR describes the status of the simulation's ability to emulate the threat at that point in time, and that there may have been changes in the threat definition or in the simulation since the VR was written. The introduction should identify a point of contact for users to gain additional information.
SECTION II VALIDATION PROCEDURES This section should identify the directives that apply to this report. It should identify the sources of data for both the threat and the simulator/target, along with the process used in determining the impacts of differences between the threat and the simulator/target that have been documented.	**SECTION II VALIDATION PROCEDURES** This section should identify the directives that apply to this report. It should identify the sources of data for both the threat and the simulation, along with the process used in determining the impacts of any differences between the threat and the simulation or any limitations of the simulation that have been documented. In addition, it should describe the assumptions, constraints, methods employed, data, tools, and techniques used to conduct the validation.
SECTION III THREAT DESCRIPTION This section should provide a brief narrative description of the threat as it is currently defined. It should also state that the data have been extracted from DIA documents or identify the other documents used as source data for the threat information. State if the DIA has approved any or all of the data that were drawn from non-DIA documents. Generally, block diagrams should be placed in appendix A rather than in this section. Operational doctrine, time sequence from Acquisition to Track to Launch to Intercept, type of system, for example, are appropriate in this section. Discussion that builds on the data provided in appendix A or provides additional explanation of the information in appendix A should be included.	**SECTION III THREAT DESCRIPTION** This section should provide a brief narrative description of the threat as it is currently defined. It should also state that the data have been extracted from DIA documents or products or identify the other documents or products used as source data for the threat information. State if the DIA has approved any or all of the data that were drawn from non-DIA documents or products. Operational doctrine, event sequences, and types of systems, for example, are appropriate in this section. Discussion that builds on the data provided in appendix A or provides additional explanation of the information in appendix A should be included.
SECTION IV SIMULATOR/TARGET DESCRIPTION This section should specifically identify all the functions of the threat that are included, and any of the functions of the threat system that are not included as part of the simulator/target. If some portions are simulated in hardware (for example, target tracker and missile seeker), while other portions are simulated in software (for example, missile fly-out), that too should be stated. It is preferred that a simulator/target system be fully addressed in one report, rather than breaking it apart into two or more reports (for example, the target tracker in one report, with the missile seeker and the fly-out model in a separate report). In many cases the simulator/target is programmable in a number of areas and could be readily changed as the threat definition changes. Significant programmability should be covered in this section. As it is also important that the programmable features cover the	**SECTION IV SIMULATION DESCRIPTION** This section should specifically identify all the functions of the threat that are included, and any of the functions of the threat system that are not included as part of the simulation. It should also describe the overall capabilities and typical uses of the simulation, the functional capabilities represented (system, behaviors, environment, and phenomenon), and the level of fidelity at which each function or object is represented. This section should also address the assumptions upon which the simulation was developed as well as assumptions pertaining to user inputs and model-generated outputs. A brief history of the simulation development and any previous validations conducted should be included. Finally, this section should describe the degree to which the software is free from error, the appropriateness and error-freeness of the data as well as any transformations used

Table Z–1
Validation report format and content—Continued

current threat estimate, the report should include that information. If there are any special modes of operation they should be described here.	to convert the data from one format to another, and the degree to which the simulation output agrees with real world objects. For the purposes of threat simulation validations, "real world" objects may include results of other standard or generally accepted simulations (benchmarking), subject matter expert review, face validation, and comparison with test data or foreign materiel exploitation data.
SECTION V DISCUSSION OF DIFFERENCES AND IMPACTS This section should address all the significant impacts on testing or training that may occur due to differences between the current threat and the simulator/target. These statements of impacts may be based on a single difference between the threat and the simulator/target, or they could be based upon a group of differences. If there are differences that tend to counter-balance the impact each may have individually, they should be discussed together. There is no need to address each difference between the threat and the simulator/target, only those that individually or collectively could be expected to have an impact on test or training results. While specific systems that have been designated to be tested against the simulator/target can be useful in identifying some of the impacts of differences, the VWG should consider all types of systems that may undergo testing with this simulator/target when they identify the impacts of differences.	**SECTION V DISCUSSIONS OF DIFFERENCES AND LIMITATIONS AND THEIR IMPACTS** This section should address all the significant impacts on testing or training that may occur due to differences between the current threat and the simulation or limitations of the simulation. These statements of impacts may be based on a single difference between the threat and the simulation of they could be based upon a group of differences, or on a single limitation or multiple limitations. This section should address limitations and conditions of applicability of the simulation to include any intentional and unforeseen limitation, limitations resulting from known but uncorrected errors, and limitations pertaining to user inputs and model generated outputs. Key to this section is a statement of the usability of the simulation for the specific systems that have been designated to be tested against the simulation as well as other types of systems that may undergo testing with this simulation.
SECTION VI CONCLUSIONS AND RECOMMENDATIONS This section should address the overall conclusions and recommendations that can be reached on the basis of the impacts of the differences between the current threat and the simulator/target. There may be several impacts that affect only one type of test, leaving the simulator/target well suited for other tests. This should be stated. It is possible that the simulator/target is so different from the threat in one or several different areas that a modification is recommended.	**SECTION VI CONCLUSIONS AND RECOMMENDATIONS** This section should address the overall conclusions and recommendations that can be reached on the basis of the impacts of the differences between the current threat and the simulation or on the limitations of the simulation. There may be several impacts that affect only one type of test, leaving the simulation well suited for other tests. This should be stated. It is possible that the simulation is so different from the threat in one or several different areas that a modification is recommended. This section should also describe any implications for simulation use.
SECTION VII REFERENCES This section should list all references used in the report. This section should list all references used in the report.	**SECTION VII REFERENCES** This section should list all references used in the report. This section should list all references used in the report.
APPENDIX A Section A1. This section should provide a key to the abbreviations used in the data entries in section A2. All the items such as NA or N/A, Nap, NSm, should be explained. Whenever the threat data has no confidence level associated with it, the report should state how data in the Confidence Level column have been coded to show that fact. Section A2. This section should contain the standard validation criteria from the appropriate appendix/annex of the DoD Threat Simulator Program Plan with all the threat simulator/target data. In cases where the simulator/target has been made programmable, do not simply state programmable. The range of programmability must be stated along with the fact that the function is programmable. If any of the programmable items have been programmed such that they do not match the current threat definition, this must also be stated. Validators' notes and threat analysts' comments should be identified in the Remarks column, and included at the end of this section. All portions of the	**APPENDIX A** Section A1. This section should provide a summary table identifying the significant entities represented in the simulation, the function of each, an indicator of the level of confidence in the representation of that entity and function and any comments. Section A2. This section should include a representative sample of the results of tests or comparisons performed as part of the simulation validation effort and as described in the simulation validation plan. Tests or comparisons that illustrate simulation errors, limitations or differences from the threat should be included as well. In most cases, these results will appear as graphs. Section A3. This section, when applicable, should contain the standard validation criteria from the appropriate appendix/annex of the DoD Threat Simulator Program Plan with all the threat simulator/target data. In cases where the simulator/target has been made programmable, do not simply state programmable.

Table Z–1
Validation report format and content—Continued

standard validation criteria should be addressed, however for those portions that do not apply, such as Continuous Wave parameters for a pulsed radar system, simply state "Not Applicable" for the header entry for that group of parameters and delete subordinate parameter numbers and names in the group from the report. The threat analyst should already have accomplished this. Do not leave out a portion of the standard validation criteria without explanation.	The range of programmability must be stated along with the fact that the function is programmable. If any of the programmable items have been programmed such that they do not match the current threat definition, this must also be stated. Validators' notes and threat analysts' comments should be identified in the Remarks column, and included at the end of this section. All portions of the standard validation criteria should be addressed, however for those portions that do not apply, such as Continuous Wave parameters for a pulsed radar system, simply state "Not Applicable" for the header entry for that group of parameters and delete subordinate parameter numbers and names in the group from the report. The threat analyst should already have accomplished this. Do not leave out a portion of the standard validation criteria without explanation.

(1) A TSP contains the narrative, pictorial, and parametric description of the threat system being simulated. It is provided by the MATDEV and approved by the appropriate IPC. Standard formats and parameter listings prepared by the former CROSSBOW committee (now identified as the Threat Simulator Investment Working Group (TSIWG)) are used as guides. The TSP contains the most current information available concerning the threat system; this information is required for section III of the VR.

(2) The System Description (SD) contains the narrative, pictorial, and parametric description of the simulator/simulation undergoing validation. The simulator/simulation developer using the same format and parameters as the TSP prepares it. Depending on the stage of simulator/simulation development, the SD contains either the most current design specifications or actual measured data from the threat system being validated. This information is necessary for section IV of the VR.

b. In order for validation requirements to comply with DoD Guidelines, validation must be accomplished throughout the threat simulator/simulation life cycle. Figure Z–4 depicts the validation events in the threat simulator life cycle.

(1) Validation of the design specification, called a DSR, establishes a means for the evaluation of the threat simulator/simulation design, the current DIA approved intelligence regarding the threat system, the projected use of the device or simulation and the simulation validation plan. Appendix F of DA Pam 5–11 provides a sample validation plan format. The completion of a DSR VR is required but is not reviewed by HQDA. The threat system developer, however, is required to submit a memorandum to TEMA stating that the DSR process has been completed and coordinated with the relevant integrated process team. The results of the DSR process will be highlighted indicating, as a minimum, that the threat system developer, the appropriate IPC, and the intended customer concur with the design of the simulator/simulation and the decision to proceed beyond the design phase. Nonconcurrences must be explained in the memorandum. General validation procedures are followed when conducting a DSR, however, no actual measurements are taken at this stage of development since there are only design specifications and intelligence data to evaluate. Every effort must be made to complete a DSR prior to proceeding beyond the design phase. Should an IOC contract be awarded prior to completion of DSR, only minimum expenditure of program dollars may be authorized, and a copy of such authorization from the Materiel Decision Authority (MDA) must be furnished to TEMA documenting the decision and circumstances pertaining thereto.

(2) Validation at IOC provides the first opportunity to compare the complete, functional threat simulator/simulation, current DIA approved intelligence estimates of the threat system, and the operational requirement for the device or software. This validation is used to support the fielding decision and documents the performance of the threat system/simulation for test planning and audit purposes. TEMA and as appropriate DOT&E, approval of the VR is required prior to simulator/simulation use in testing and where resulting data will be used in a report or otherwise to support a milestone decision by the appropriate MDA. The IOC validation is the final validation prior to fielding the system/simulation; therefore, it is based on actual measurements (simulators) or data generation (simulation) and the most recent intelligence data. IOC is the most complete and thorough validation a system/simulation will undergo since it is essential at this point to confirm and define the differences between actual measured simulator data or simulation-generated data and the DIA approved threat data.

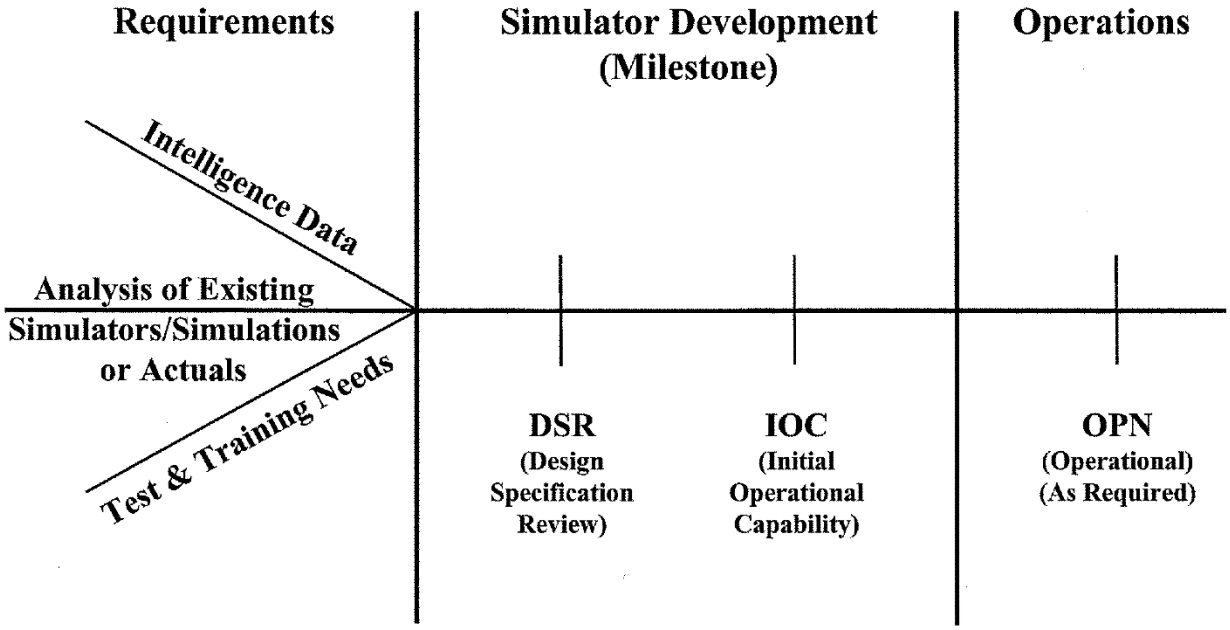


Figure Z–4. Validation events in the life cycle of threat simulators/simulations

(3) A periodic review is conducted on all legacy simulators/simulations to determine the need for an operational (OPN) validation. An operational validation is required on all threat systems/simulations after major modifications, significant changes to the intelligence data, or a significant change/degradation to the simulator/simulation to document their continued capability to represent threat systems as described by current intelligence estimates. The IOC VR will recommend critical parameters and intervals for OPN reviews. The VWG chairperson will review the recommended intervals as well as the critical parameters to be considered. OPN validations consist of comparison and analysis of simulator/simulation performance, configuration, and fidelity to current threat estimates. Actual simulator measurements and/or simulation-generated data will be used in OPN validations but only for the critical parameters. The simulator/simulation/target MATDEV representatives, in coordination with the OPN VWG, may be required to designate/select the critical parameters if they have not previously been identified. For those systems, the first OPN VR may require a more extensive critical parameter list and other descriptive data to adequately establish the baseline information normally found in an IOC VR.

c. The general validation process requires the design, engineering and technical limitations of the threat system/simulation and its projected use be reviewed. To accomplish this review, the combined expertise of the intelligence community, the target or threat simulator/simulation developer, developmental and operational testers is required. Accordingly, a VWG composed of representatives from the above organizations will constitute the primary Army validation organization.

(1) During the engineering and technical analysis process, the design, engineering and technical characteristics and capabilities of a threat simulator/simulation (as outlined in the SD or other related document) are analyzed and compared to current DIA approved threat intelligence (as outlined in the TSP or other threat related document) for the related threat system. The results of this process will be documented in section V, and summarized in section VI, of the VR.

(2) An operational analysis is also accomplished by the VWG. It compares the capabilities and limitations of the threat simulator/simulation as found during the design, engineering and technical analysis, with the threat's operational characteristics to ascertain its performance capabilities. Details from this operational analysis will also be discussed in section V and summarized in section VI of the VR.

d. VWGs will evaluate and report on threat targets or threat simulators/simulations at the required points in the life cycle identified in paragraph Z–10*b* (Validation Requirements).

(1) A VWG will be established and chartered for each target or threat simulator/simulation, and usually for each validation requirement. TEMA will charter VWGs based on schedules provided by PM ITTS. The charter will establish TEMA as chairperson and designate the organizations to participate in the VWG.

(2) Generally, VWGs are composed of representatives from the responsible user, IPC, PM ITTS, and the simulator/simulation or target development organizations. Representatives from the following organizations will participate in VWGs as indicated:

(a) Mandatory members include representatives from ATEC, the appropriate IPC for the systems involved, U.S. AMSAA, PM ITTS, DCS, G–2, and the Threat Simulator or Target developer (if other than PM ITTS).

(b) Additional members as required include ARL, AMC Research Development and Engineering Centers, TRADOC, PEO/PM (appropriate blue systems), other Army organizations, and other DoD representatives as deemed necessary by the VWG chair. General functional areas and organizations, as well as general membership are shown in figure Z–5. The events involved in validation are illustrated in figure Z–6. The functions and responsibilities of the VWG are discussed below.

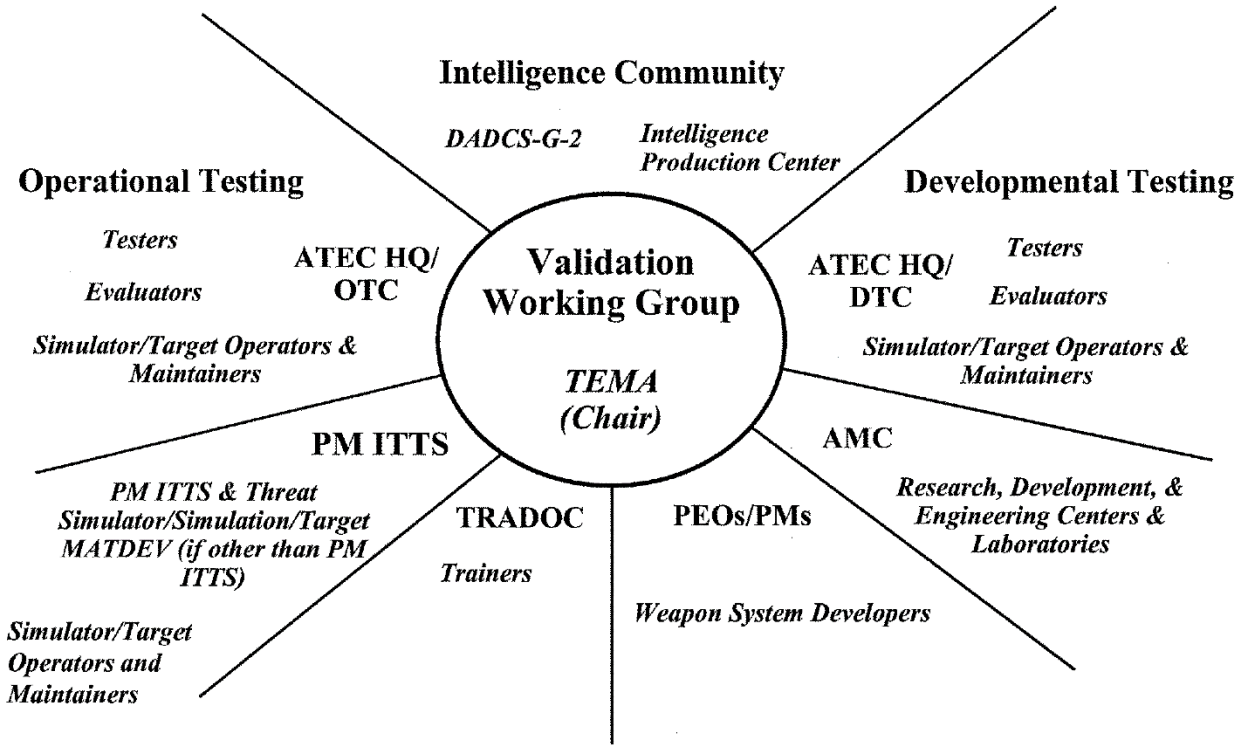


Figure Z–5. Validation working group membership pool

(c) The DOT&E approved standard validation criteria cover a broad spectrum of parameters that describe threat systems. Upon establishment of a VWG, the threat system MATDEV representative, in coordination with the IPC representative, will tailor a set of standard validation criteria for use in validating the simulator/simulation in question. The proposed criteria will be drawn from approved DOT&E standard validation criteria and may be augmented if required. The VWG will ensure that the standard validation criteria (parametric listings) describing threat equipment are used for both the TSP and the SD. If DOT&E approved standard validation criteria are not available, the simulator/simulation or target MATDEV, in coordination with the IPC, will develop a proposed set of criteria to be used for the validation. The coordinated proposed validation criteria will be forwarded to the VWG chairperson for approval, and to DOT&E for information. The same standard criteria will be used for DSR and IOC validations.

(d) Design, engineering, technical, and operational analyses will be conducted by the VWG.

(e) Information will be documented in a VR.

(f) VWG will submit the required VR for approval (at IOC) or for notification, information, and retention (at OPN) to DOT&E. The VR should be forwarded using a letter of transmittal. The VR parametric data format and simulation summary reports are illustrated in tables Z–2 and Z–3, respectively (sample only; no actual data shown).

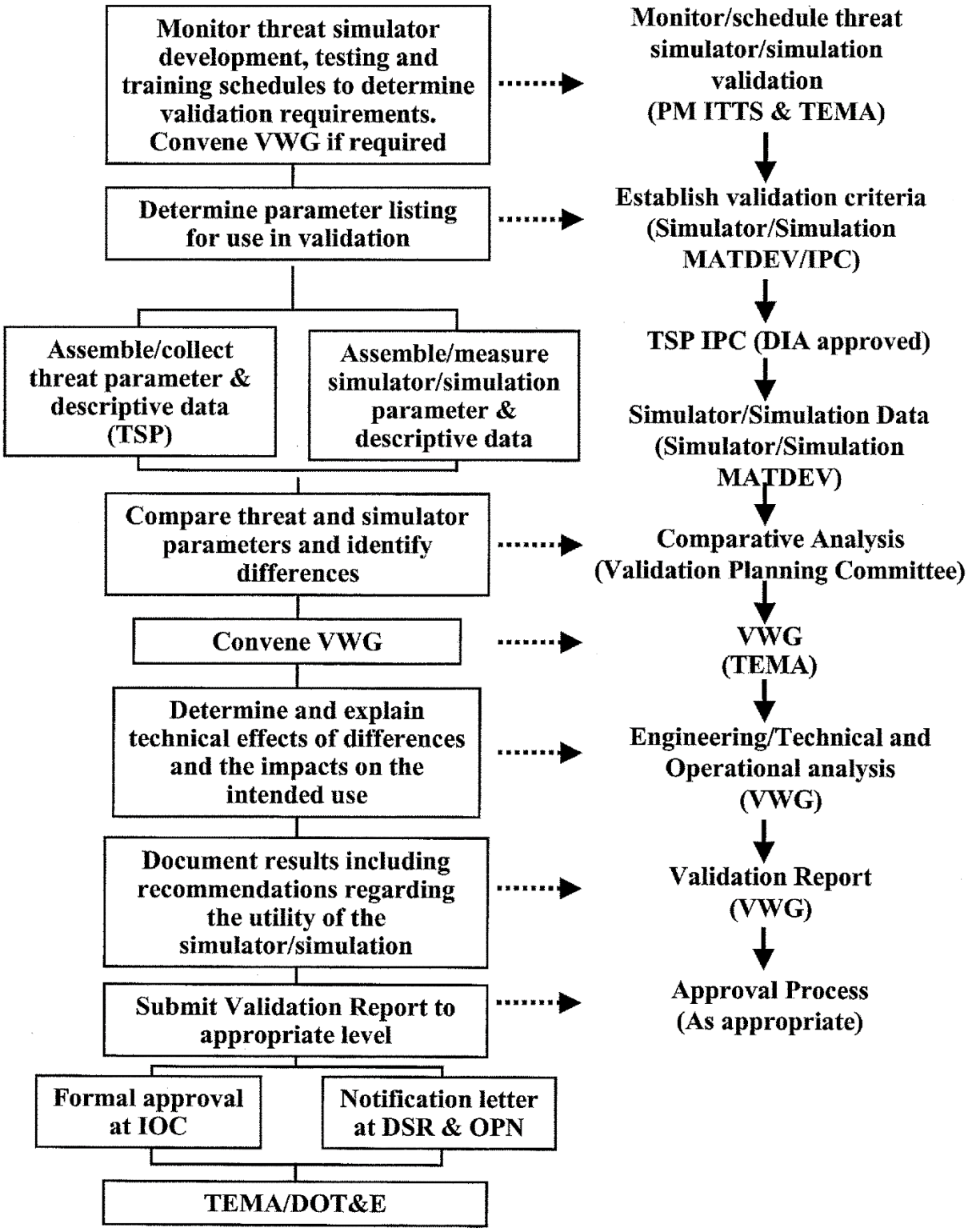


Figure Z–6. Validation event cycle

Table Z–2
Sample simulator/simulation validation report parametric data format—Continued

Crossbow #	Subsystem/ parameter	Units	DIA threat estimate low-most-high	Simulator/ simulation target value	Remarks	Deltas	Impact
J1.1	RF communications	Yes/No	No	No			
D2.223.5	RF power out	Watts	5	3	Rem2	2	D1
R4.234.7	Antenna length	Meters	1:1.5	Nap		Yes	F4
			2:4	Nap		Yes	F4
			3:3	Nap		Yes	F4
P3.3	Polarization	Text	Vertical	Vertical			
F1.2.3.5	Antenna type	Text	Whip	Log period		Yes	A3
C1.0	Number of bands	Integer	1	1			
P3.4.5	Radiated power	dBW	50 to 60	70		10	D3

Table Z–3
Sample simulation summary report

Entity	Function	Confidence	Comments
Target Acquisition Radar (TAR)	Detection	No clutter - High Clutter - Medium	Simulation of the TAR operating in a no-clutter environment produces results consistent with FME.
TAR	Detection	Clutter - Medium	No data are available to validate simulation results for a clutter environment.
TAR	Mode Logic	High	Consistent with FME findings and intelligence information
	Waveform Logic	High	Consistent with FME findings and intelligence information
Target Tracking Radar	Track Accuracy	No Clutter - Medium	No actual test data available, however, track errors are lower than engineering analysis assessments
Target Tracking Radar	Waveform Usage	High	Consistent with FME findings and intelligence information. Target tracking radar wobulation mode is not modeled due to limitations in the Joint Modeling and Simulation System signal packet.
Weapon Controller	Launch solution	High	Consistent with FME findings, except that the missile launch solution does not observe 300 m/s launch limit on outbound targets.

(g) Threat simulators/simulations developed and fielded prior to implementation of DoD threat validation procedures were not subject to the developmental validation process, such as the DSR and IOC validations. They are, however, subject to the provisions for OPN validation. For those systems, the MATDEV, in conjunction with the user or the owning organization, and the responsible IPC will determine the OPN validation cycle. The resulting schedule will be forwarded to TEMA, who will then establish and notify members of the OPN VWG. If critical parameters for OPN validations have not previously been developed, the MATDEV, in conjunction with the user or the owning organization, and the appropriate IPC will develop a list of critical parameters and forward them to the VWG chairperson for approval. Any unresolved issues regarding OPN validations will be sent to TEMA for resolution.

(h) The VWG will determine an appropriate location for the conduct of the OPN validation. The VWG will base its decision on a thorough review of changes in the threat and other pertinent factors that may impact the amount of

effort involved in conducting the OPN validation. The VWG will then select the most convenient, least disruptive (to testing), and least expensive location suitable for the conduct of the OPN validation measurements.

e. The VWG Planning Committee assists the VWG in its mission to ensure all threat systems are validated prior to accreditation and use. In its role as chair, PM ITTS will—

(1) Chair a minimum of two planning meetings per year, alternating with the semiannual DA VWG meetings. Additional meetings may be necessary to support VWG activity and assist TEMA in the execution of its Army Threat Systems/Simulation Validation responsibilities. Typically meetings are scheduled as follows:

(a) VWG Planning Meeting April.

(b) VWG Late May.

(c) VWG Planning Meeting August.

(d) VWG Early November.

(e) VWG Planning Meeting December.

(f) VWG March.

(2) Solicit attendance to the Planning Committee meetings as warranted. Members of the planning committee will normally be representatives of the core VWG membership. A representative from TEMA will attend these meetings to provide program guidance and present the DA perspective relative to agenda items and the ensuing discussions pertaining thereto.

(3) Conduct planning meetings to—

(a) Address VR issues prior to consideration by the VWG.

(b) Develop validation goals and objectives based on known test events requiring validated threat assets.

(c) Develop, and annually publish, a validation schedule with required updates as warranted throughout the year to ensure currency and accuracy.

(d) Ensure that the AMC ATSMP is crossed-walked with the validation schedule to ensure accuracy. Review accreditation schedules to ensure planned system validations are being conducted in sufficient time to provide necessary data in support of ATEC's threat system accreditation program. Annually canvass the acquisition and T&E communities to further identify threat system validation requirements.

(e) Provide quarterly validation schedule change updates to the VWG membership in conjunction with the preplanned meetings cited above. If these meetings are not held, a quarterly updated change report, if required, will be forwarded to the VWG membership.

(4) Provide recommendations to TEMA on validation waiver requests.

(5) Provide planning committee meeting minutes to TEMA within 30 days after the conclusion of the meeting.

(6) Participate in OSD VWG forums as required.

f. It is essential to keep the validation process as simplified and non time-consuming as possible without degrading the quality of the reports. Content rather than appearance should be the primary focus.

(1) Table Z–4 outlines the procedures for systems undergoing DSR and IOC validations.

Table Z–4
Threat simulator/simulation design system review and initial operational capability validation report

Item	Procedures
1	PM ITTS monitors and coordinates TSP requirements and validation schedules and submits data to TEMA.
2	TEMA coordinates and transmits TSP requirements with DCS, G–2 and TSIWG.
3	TEMA charters a VWG. If required, a planning and coordination meeting will be convened to establish the validation parameters listing.
4	The appropriate IPC provides or produces the TSP and forwards it to the VWG chairperson.
5	Simulator developer produces the system description document. Simulation developer produces a functional requirements document and validation plan.
6	Under the direction of the VWG chairperson, the MATDEV produces a document listing the validation parameters, threat values, simulator values or simulation-generated data, and the delta between the threat and simulator or simulation-generated values.
7	VWG analyzes the design, engineering and technical implications regarding the deltas of the capabilities of the simulator or simulation.
8	TEMA or a designee convenes and chairs the VWG, which will normally be scheduled as 1-day meetings. The analysis is reviewed and final coordination completed. The VR is signed by all VWG members and when appropriate, forwarded

Table Z–4
Threat simulator/simulation design system review and initial operational capability validation report—Continued

	to the TSIWG chairperson for approval.

Notes.
[1] The VR contains the following—Validation and simulator/simulation parametric values, threat parametric values, and the parametric deltas between the threat and the simulator/simulation. Analysis outlining the design, engineering and technical impacts of the parametric deltas between the threat and the simulator or simulation regarding the actual operation of the simulator. Analysis outlining the impacts on testing of the parametric deltas. Cover letter forwarding the report with the results of the analysis and recommendations concerning continued development or additional data requirements or modifications. IOC VRs contain critical parameters and time intervals between operational validations.

Table Z–5
Operational validation process[1]

Item	Threat simulator/simulation operational validation process
1	PM ITTS monitors/coordinates operational validation schedules and provides to TEMA. If not previously designated, PM ITTS, in coordination with the simulator/simulation owner, and the appropriate IPC, will recommend to TEMA critical parameters and schedules for use in operational validation.
2	TEMA coordinates operational validation requirements with DCS, G–2 and the TSIWG.
3	The appropriate IPC approves the updated TSP developed by the MATDEV for the critical operational parameters only.
4	The owning organization will provide updated descriptive data and measurements of the critical operational parameters (that is, modified simulator data to match the modified TSP) to TEMA and PM ITTS.
5	TEMA/PM ITTS determines whether or not a full VR is required. This decision is based upon an analysis of both the updated threat and simulator data to determine if significant changes have occurred. If significant changes have not occurred, TEMA coordinates a statement to that effect with the VWG membership. This completes the operational validation process.
6	If significant changes have occurred, PM ITTS, in conjunction with TEMA, directs the conduct of an operational validation.
7	TEMA or a designated organization convenes and chairs the VWG. Based on actual measurements of the threat system's critical parameters, the VWG analyzes and compares the threat system performance, configuration, and fidelity to current threat estimates.
8	The results of the comparison and analysis are documented by the simulator/simulation owner and forwarded to TEMA.

Notes.
[1] Operational validations may be limited to one page of statements indicating no significant deltas exist between the critical parameters of the threat system and current threat estimates. This one page is attached to the last VR to serve as an updated operational validation.

(2) OPN validation procedures are designed for systems already fielded and are a modification of the general validation procedures. Table Z–5 outlines the procedures for OPN validation. The operational validation is concerned only with the critical parameters. The owning organization will provide to TEMA updated simulator/simulation/target data and updated threat DIA approved intelligence from the IPC. TEMA will determine if a full operational VR is required. The decision will be based on an analysis of both the updated threat and simulator/simulation/target data to determine if significant changes have taken place that concern the critical parameters. If it is determined that significant changes have not taken place, TEMA will coordinate with the VWG members to sign off on a statement to that fact. The statement is attached to the front of the most recent VWG report and serves as an updated operational validation. If significant changes have taken place, the owning organization will produce an abbreviated VR (limited to the critical parameters) and the general validation procedures will be followed.

(3) Special procedures for validation of Programmable Threat Simulators (PTS). Validation of PTS will be in accordance with a three-phased process negating the need for costly, repetitive validations. The intent is to reduce the cost associated with validating PTS, without compromising the validity of the threat representation utilized in testing. The three phases are—

(a) Phase I—Establish Limits and Diversity Characteristics. The first step is to establish a list of critical validation parameters for the specific PTS based upon the critical threat parameters. The Army VWG then convenes to review

and approve the list of critical validation parameters for the PTS. Once approved, the limits and diversity characteristics of the PTS critical parameters will be established through testing.

(b) Phase II—Demonstrate Programmability. The second phase is to demonstrate the programmability of the PTS. A small sample of threat systems (3 to 5) will be chosen to demonstrate the capability of the PTS to replicate various aspects of the selected threat systems. The sample size should be proportional to the complexity and diversity of the PTS, with threat systems chosen to demonstrate the limits of the PTS wherever possible. The PTS will be configured to replicate each threat system in the sample group. Parametric measurements will be taken and the resulting data compared to the DIA approved intelligence data for the corresponding threat system. Any differences that exist between the simulator data and the threat data will be analyzed to determine potential impacts or limitations on simulator usage. These measurements should be conducted in conjunction with the measurements required in Phase I.

(c) Phase III—Documentation and Approval. The final phase of the process is the documentation and approval phase. Data and information gathered in the first two phases will be compiled in a PTS VR. The format for this report is the same as used for other VR, although some changes may be required based on the individual PTS. While a standardized format is desired, the focus of the report will be the presentation of the relevant data and information, including a comparison matrix (Standard Validation Criteria Tables) with identified differences and potential impacts discussed. Once a Draft PTS VR has been completed, it will be presented to the Army VWG members for review and approval in accordance with AR 73–1. After the Army VWG has approved the PTS VR, the VWG will recommend that the PTS be validated as a threat simulator for all threat systems whose critical parameter values fall within those of the PTS performance parameters. As with all threat simulator reports, TEMA's Director will approve the PTS VR and forward it to DOT&E for final approval as required. Once approved, the PTS is authorized for use in support of testing until the next scheduled operational validation review.

(4) Foreign materiel validation procedures are a modification of the threat simulator/simulation/target validation process. Foreign systems are generally exploited or baselined by the IPC. Baseline or exploitation data will be made available to the VWG by the IPC. When available, the IPC exploitation report will be used by the VWG as the basis for validation of the exploited system. For actual systems where no intelligence data exist, the measured data will be approved by the IPC and used to establish the threat baseline. Certification is designed simply to verify the authenticity of the threat and to document any shortcomings, degradations, or modifications to the system. Certification Reports for actual systems may be used in lieu of VRs for the accreditation process.

(a) If an actual threat system is to be used as a surrogate for another threat, (for example, a T–72 tank used to represent a T–80 tank), the surrogate will be subject to the validation and accreditation procedures outlined in this document.

(b) Actual threat systems will be considered validated after completing the certification procedures outlined below.

1. The MATDEV will coordinate the development of a list of critical parameters necessary to adequately identify and describe the threat system undergoing certification. As a minimum, concurrence from the appropriate IPC and user will be received. To the extent possible, the parameter listing should be in DOT&E's authorized format to facilitate documenting the configuration of the actual threat system.

2. The MATDEV will obtain DIA-approved system specification data from the appropriate IPC for the type system undergoing certification. The MATDEV will then extract the necessary threat values for the certification parameter listing previously developed for the system. Additionally, the MATDEV will extract sufficient descriptive data to provide a short narrative description and overview of the system and its capabilities. Where possible, information concerning any variants of the system should be included (for example, how an A model differs from a B model). All data sources will be properly documented.

3. PM ITTS will inspect the actual threat system undergoing certification and verify that the parametric data values obtained from DIA sources are present on the actual equipment. Any differences noted will be documented. Draft impact statements will be prepared reflecting any potential test or training limitations caused by the deltas. Parameters that may not have been addressed during the validation process and are considered critical to a particular tester will be measured and compared to DIA approved intelligence data during the accreditation process for that test.

4. The completed certification report (parameter listing, descriptive data, and impact statements) will be staffed with the appropriate IPC and user then forwarded to TEMA for approval. If necessary, a VWG meeting will be held to finalize the comments. A copy of the certification report will also be forwarded to the TSIWG chairperson for information purposes.

5. Certification reports will be maintained as part of the maintenance and usage records of the equipment. Organizations owning actual threat systems are responsible for ensuring that any changes in the actual threat system configurations are properly documented. The MATDEV, in conjunction with the owning organization and the responsible IPC, will periodically review the changes and make recommendations to TEMA regarding the need for recertification or possibly an OPN validation.

Z–11. Validation of targets

a. Overview of the general target validation process.

(1) Target validation will be accomplished and documented by a VWG. Due to the specificity and uniqueness associated with signature development, many of the generic aspects of validation are not applicable. The procedures for validation and accreditation of targets will be modified as outlined in this section.

(2) Target developments generally fall into two broad categories. First, there are generic targets used to represent a wide range of similar type threats. An example of this type target would be the MQM 107 used to represent subsonic fixed wing aircraft. Second, there are targets (which could include actual systems) designed to represent a single threat, with signature replication to meet specific testing milestones. For each of these cases, the validation can be streamlined by making modifications to the procedures outlined for threat simulator/simulation validation.

(3) For all targets projected for use in training or testing that will support a milestone decision, validation will occur at DSR and IOC. OPN validations are required periodically throughout the life cycle or after major modifications that affect target fidelity or alter the signature of the target, such as the addition of reactive armor or an engine upgrade. This is normally required only for targets representing a specific threat.

(4) All target VRs will be forwarded to TEMA for approval. DSR validation will be completed during target development and comply with the same procedures as identified above for threat simulators/simulations. IOC reports will be approved prior to a target being used to support a milestone DR. The target MATDEV is responsible for funding validation.

b. The target validation process. The target validation process described in this section is shown in figure Z–7.

(1) Generic targets are defined as targets not designed to represent a specific threat. They are generally used to portray a family of threats such as fixed wing subsonic aircraft and rotary wing aircraft. These targets are often augmented with add-on kits to meet specific signature requirements for a given test. These types of targets will be baselined, which is simply the description, measurement, and documentation of the key parameters associated with the physical and operational characteristics of the target. Examples of the types of information documented include, but are not limited to, the length, width, weight, maximum speed, maximum altitude, and turning radius. The purpose of baselining is to provide sufficient data to the tester/developer so they can determine if the target will meet their general requirements. Separate appendices should be included in the baseline report to describe any augmentation kits that can be attached to the generic target. Generic target baseline reports will be prepared and approved by the target MATDEV and an information copy forwarded to the Director, TEMA. All comparisons of generic type targets to specific threats will occur during the accreditation process. Target accreditation will follow the accreditation procedures outlined for threat simulators/simulations.

(2) Threat specific targets will follow a modified threat simulator validation process as outlined below. As an exception, threat specific targets that do not portray electronic signature data (such as only visual and performance characteristics) will be validated according to the threat simulator/simulation procedures described in paragraph Z–10 (validation of threat simulators/simulations). Infrared, millimeter wave, seismic, and acoustic data are considered electronic. The MATDEV representative, in coordination with the IPC representative, will tailor a set of standard validation criteria for use in validating the threat in question. The proposed criteria will be drawn from approved DOT&E standard validation criteria and may be augmented if required. The VWG will ensure that the standard validation criteria (parametric listings) describing threat equipment, prepared from the listings approved by DOT&E, are used. If DOT&E approved standard validation criteria are not available, the MATDEV, in coordination with DOT&E and the IPC, will develop a proposed set of criteria to be used for the validation. The coordinated, proposed validation criteria will be forwarded to the VWG chairperson for approval. The same standard validation criteria will be used for DSR and IOC validations.

(3) Signature data for threat specific targets will be validated as indicated below.

(a) The specific signature requirements for known tests will be collected.

(b) Signature parameter definitions will be developed by the supporting IPC.

(c) Threat signature data will be collected or developed by the supporting IPC in accordance with the developed parameter definitions and the approved test requirements. approved test requirements. The MATDEV will arrange for the appropriate organization to conduct the target signature measurements. The MATDEV and other members of the VWG will complete an engineering and technical analysis, comparing the target and threat signature data. Complete actual signature measurements are possible only at the IOC validation point. For DSR, the results of the engineering and technical analysis, along with any other relevant information will be evaluated. Maximum effort should be made to utilize advanced M&S techniques to predict signature replications. The results of the engineering and technical analysis will be documented in section V and section VI of the VR.

(d) Target signature data will be measured in accordance with the parameter definitions.

(e) The VWG will compare the capabilities and limitations of the target with its operational use to determine the target utility, complete the VR, and submit it to TEMA for approval.

(f) All future signature data requirements for the validated target will be reviewed, developed, and approved as part of the accreditation process.

(4) Actual foreign equipment utilized as targets should follow the procedures outlined in paragraph Z–10*f*(4). Any additional data required for training or testing should be documented as part of the accreditation process. Procedures outlined for threat simulator accreditation should be followed.

(5) Joint use targets will require approval by TEMA and DOT&E.

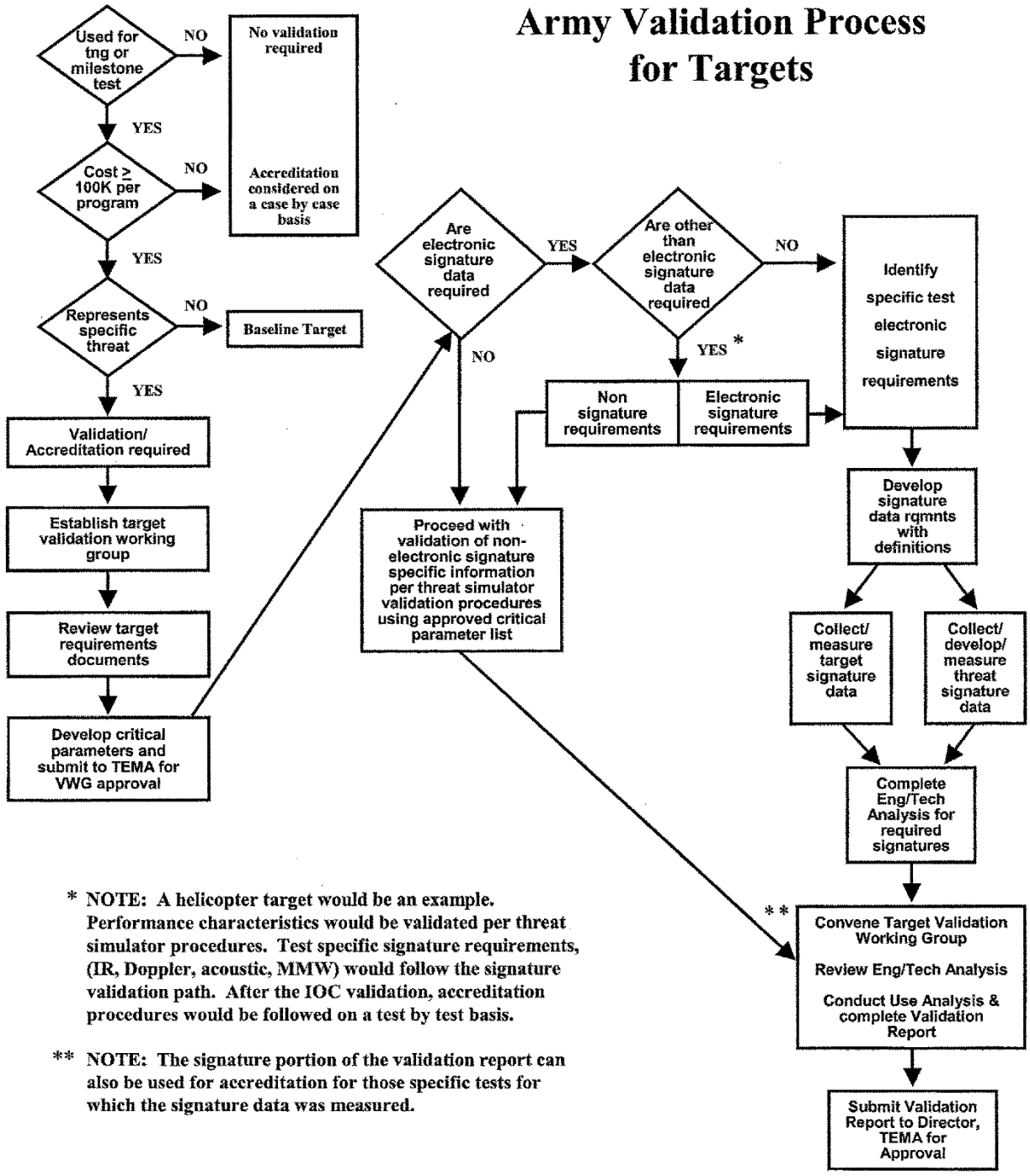


Figure Z–7. Army validation process for targets

Z–12. Accreditation

a. Accreditation is the process used to determine whether threat simulators/simulations, surrogates, actual threat systems, and targets are suitable for a specific test. The data requirements are compared to the latest intelligence and the capabilities of Army threat simulators/simulations and targets as shown in current VRs. In cases where VRs are not available, or where other constraints make validation unfeasible, waivers will be handled on an exception basis. All requests for exceptions/validation waivers will be forwarded to TEMA for approval. ATEC will not proceed to

accredit threat systems for OT testing unless a waiver for validation has been approved by TEMA. Accreditation examines any parametric differences to determine their impacts on the test or training application. A complete validation of a threat system prior to accreditation/OT testing should provide sufficient documentation of the threat system's operational status, permitting analysts to quickly eliminate or include the threat system performance or its overall condition as a contributing factor to a failed test event by a system under test. To assist in projecting validation actions, ATEC will publish an annual accreditation schedule that is updated 6 months from publication to reflect cancelled or added test programs. The accreditation event cycle is depicted in figure Z–8. General functional areas for organizations participating in accreditation are outlined in figure Z–9.

(1) Threat accreditation is essential for the following reasons:

(a) Any differences between a threat simulator/simulation/target and the corresponding actual threat system can distort representation of the threat. Even the differences accepted during development and validation can make the simulator/simulation or target incapable of adequately representing the threat for a specific test or training exercise.

(b) The intelligence concerning threat systems is dynamic. New intelligence can make a simulator/simulation or target inappropriate for a given test or training application.

(c) Threat simulators and targets experience deterioration and failures that can render them no longer threat representative. Models and simulations often require updates due to intelligence data, operating system or compiler changes. Accreditation decisions, therefore, must be based on current assessments of the performance of the simulators/simulations and targets.

(2) Accreditation for testing is accomplished under the auspices of the weapon system PEO/PM whose system is undergoing test and is documented in support of the weapon system T&E WIPT. Responsibilities for accreditation costs will be in accordance with AR 73–1. Threat simulator/simulation, target, and test usage requirements will be identified in sections 4 and 5 of Part V of the system TEMP. These paragraphs should include the number, type, and fidelity requirement, compare threat requirements, and note the shortfalls.

(3) Accreditation is required for any testing where the data will be used to support milestone DRs. For OT, the accreditation process complements the function of the TCG and T&E WIPT (to include the threat subgroup) to improve test planning by specifically defining test resource requirements for the specific application in the OTP, which must be submitted for approval to the TSARC before test design and threat support planning can be fully documented. For all testing, TCG and accreditation affords an early opportunity for the weapons system MATDEV, evaluator, tester, and threat manager or foreign intelligence officer to coordinate respective test planning efforts.

(4) For OT, the process should be accomplished to allow timely inclusion of accredited threat simulator/simulation and target resource requirements in the final OTP for approval by the TSARC. TSARC policy requires at least a 2-year lead-time between TSARC approval and first allocation of personnel and equipment from an external organization (see AR 15–38). An in-cycle OTP must be submitted to ATEC for review and staffing 9 months before its presentation to the TSARC.

b. TAWG membership and responsibilities are described as follows:

(1) TAWGs will be established under the auspices of the T&E WIPT by the PEO/PM whose weapon system is being tested. For all tests of ACAT I, ACAT II, or any other system on the OSD T&E oversight list ATEC will either chair or designate a TAWG chair. Records of DT and OT TAWGs should be maintained by the appropriate ATEC Support Team (AST) chair to ensure threat consistency throughout testing. For ACAT III programs not on the OSD oversight list, ATEC will designate the TAWG chair with the assistance of the AST chair. The chairperson of the T&E WIPT for each program will coordinate with the ATEC Threat Coordination Office to have a TAWG chairperson appointed; subsequently, the TAWG membership will then be notified that the TAWG is established and its chairperson appointed. Future TAWG direction will come from the TAWG chairperson. A TAWG determines if the simulators/simulations and targets proposed for a specific test have the capability to represent the relevant threat characteristics needed during that test. All parties to the test planning process, particularly the threat proponents, must be aware of the requirement to accredit targets and threat simulators/simulations and share responsibility to notify the T&E WIPT/AST chairs, as early as possible, of the need to establish a TAWG. All parties to the test planning process also must be aware of the requirement that all threat-specific targets, generic targets with threat-specific components, and all threat simulators/simulations have a validation requirement and must notify the ATEC Threat Coordination Office through the T&E WIPT/AST chairs, as early as possible.

(2) TAWGs will be composed of representatives from the responsible PM, PEO, T&E WIPT, intelligence, threat simulator, and target developmental or operational organizations. Representatives of the following organizations will participate as determined by the chair, DCS, G–2/TISO, TRADOC (designated threat manager or TRADOC DCS, G–2), ATEC (tester and evaluator), AMC, AMSAA, appropriate IPC, MATDEV for threat simulator or target, ARL, appropriate PM/PEO, and others as required.

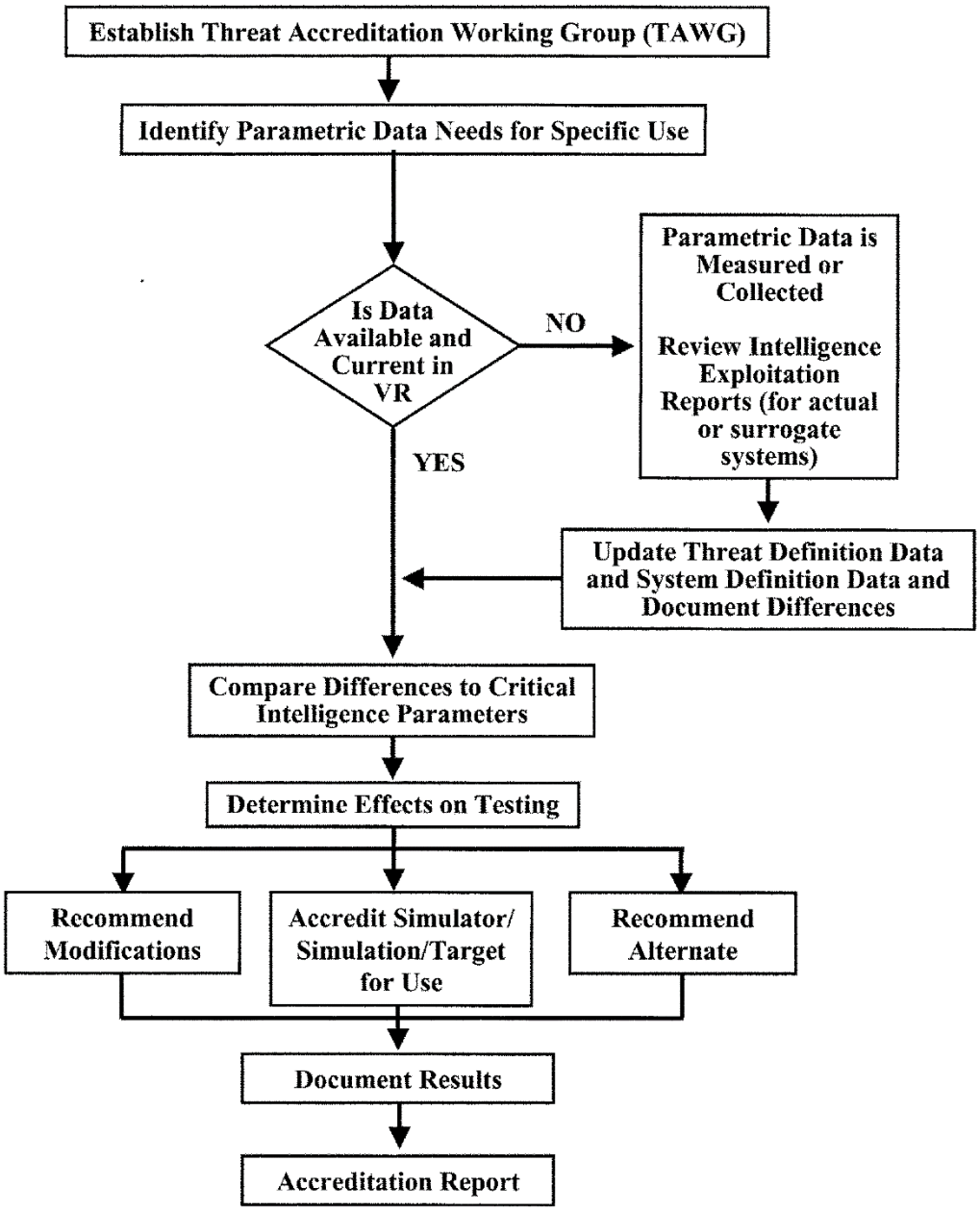


Figure Z–8. Accreditation event cycle

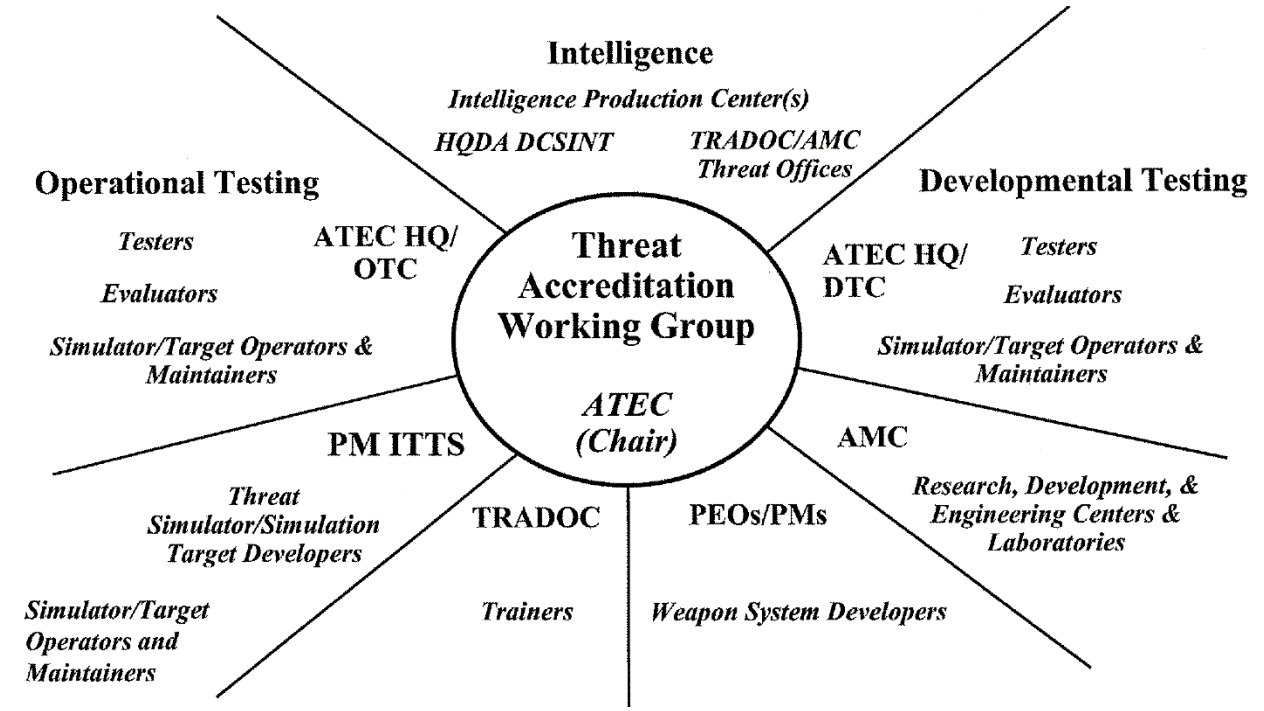


Figure Z–9. Threat accreditation working group membership pool

(1) The TAWG will review the technical requirements for the threat simulators and targets, and the simulator/simulation and target validation data, to determine the capability of the simulator/simulation and target to represent relevant system characteristics for the test under consideration.

(2) The TAWG will document, via an accreditation report to the T&E WIPT, the suitability of the individual threat simulators/simulations and targets for use in support of the specified test under consideration. A letter of transmittal (fig Z–10) will be used to forward the report to the T&E WIPT chair. Where more than one threat simulator/simulation or target is being accredited for the same test, the findings regarding each may be combined into a single report and forwarded to the T&E WIPT chair using the same transmittal letter.

(3) Due to the diverse nature of issues that may be addressed during accreditation, a standard report format is not provided. The content of the transmittal letter serves as a guide for what should be contained in the accreditation report.

(4) The following procedures should be followed by the TAWG:

(a) TAWG members first identify specific parametric data needs to satisfy the COIC for the planned testing. The threat simulator/simulation/target developer, or simulator/simulation/target owning organization, for systems already fielded, will verify that all parametric data provided in the VR are current. Any required data not included in the VR must be collected or measured as part of the accreditation process. The TISO will coordinate the verification and update of applicable parameters (characteristics and capabilities) of the threat system. The threat simulator/simulation and target developer, or simulator/simulation/target owning organization, for systems already fielded, will verify or update the same parameters of the corresponding threat simulator/simulation or target. The TAWG documents the differences between the simulator/simulation or target and the threat in a preliminary accreditation report.

(b) For generic targets or targets not previously subjected to the validation process, which will be used to represent a specific threat for a given test, the responsible MATDEV must provide the TISO with documented system parameters for comparison with the intelligence on the corresponding threat system. These parameters should consist of only those necessary to support the particular test or training scenario for which the system is to be used. For actual threat systems and surrogate systems, the TAWG IPC member may use intelligence exploitation, validation, certification, or baseline reports. The parametric on the threat system and those of the corresponding threat simulator/simulation and target, and the differences between them, will be formally documented by the TAWG in the accreditation report.

[CLASSIFICATION]

TO [CHAIRMAN, APPROPRIATE T&E WIPT]
SUBJECT: [Name of Threat Simulator / Target Accreditation Report]

1. Provide the title of the threat simulator/simulation(s) or target(s) being accredited.
2. Identify the applicable test event by title and Test Schedule and Review Committee (TSARC) number.
3. Identify the working group charter by issuing headquarters, title and date. Append a list of the working group membership.
4. Identify, by title and date, the DIA Threat Estimate used for the report preparation.
5. Parameters are only referenced in the transmittal letter, with details contained in the subject report. The report should include CIP as defined in AR 381-11, user required critical operational characteristics and capabilities as defined in the requirement document, and applicable Standard Validation Criteria.
6. Data collection/analysis is summarized in the transmittal letter, with details contained in the subject report. The report should itemize any data collection/analyses conducted (by whom, when, and where) to determine the suitability of the simulator or target to support the critical issues and criteria of the test being supported.
7. A brief summary of the major results of the data collection/analysis should be in the transmittal letter. The full report should provide full results, plus identify differences and the effect on simulator/target capability.
8. Only differences with a significant impact on testing or training need to be mentioned in the transmittal letter, with all remaining differences discussed in the subject report.

SIGNATURES: All appointed members of the TAWG

[CLASSIFICATION]

Figure Z–10. Accreditation report letter of transmittal

(c) Differences between the threat simulator/simulation or target and the intelligence concerning the capabilities of the relevant threat system must be assessed against the critical intelligence parameters (CIPs) to determine whether the performance characteristics representing the threat are within the CIPs established by the system program manager. Differences, particularly those that breach CIP thresholds, that cannot be accommodated or offset in test planning are defined and assessed to justify modification of the simulator/simulation or target, or acquisition of alternate simulators of targets. Differences assessed to breach CIP thresholds and impact on the effectiveness, survivability, and cost of the U.S. systems under development must be reported to the T&E WIPT with recommendations.

(d) Collectively, the TAWG assesses the differences between the threat simulator/simulation or target and the intelligence concerning the capabilities of relevant threat system in the context of test data requirements to determine the impacts on the test, including test limitations. These differences are then documented in the accreditation report.

Section III

Roles

Z–13. Instrumentation requirements role

a. ATEC—

(1) Provides identification of, documentation for, and adjustment to requirements for Instrumentation, Target, and Threat Simulator Program plan processes.

(2) Provides empowered representatives to participate on appropriate working groups as required.

(3) Provides coordinated ATEC priorities, project descriptions, and financial estimates on major instrumentation requirements.

(4) Provides coordination and support of all ATEC ITTS programs throughout program development plans and funding cycles.

(5) Executes sustaining instrumentation programs.

(6) Biannually sponsors the ATEC Test Instrumentation Conference. Participants include ATEC, ATEC subordinate command, OSD, PM ITTS, and other invited agencies as it pertains to the focus topics of each conference.

b. SMDC—

(1) Provides empowered representatives to participate on appropriate working groups as required.

(2) Provides coordination and support of all SMDC major instrumentation programs throughout the program development plans and funding cycles.

(3) Executes sustaining instrumentation programs.

c. PM ITTS—

(1) Develops, acquires, fields, operates and maintains, and provides life cycle management of Army targets, threat simulators/simulations, and selected major test instrumentation except those designated by regulation to other Army agencies, such as SMDC.

(2) Provides empowered representative participation to ATEC's instrumentation, targets, and threat simulator/simulation requirements processes.

(3) Gathers and integrates Army test requirements into a shared, Army-wide approach to ITTS investment.

(4) Provides coordination and contact with ATEC regarding all ATEC instrumentation, targets, and threat simulator/simulation requirements and the execution of projects against those requirements.

(5) Establishes working groups for each major instrumentation, target and threat simulator/simulation program. Participants will include, PM ITTS, TEMA, ATEC, and appropriate representation from ATEC subordinate commands as required and determined by ATEC.

d. ATEC and PM ITTS jointly—

(1) Ensures that all ITTS investments in both commands are regularly reviewed and updated as cost, schedule, or performance requirements change or as funding available for execution changes.

(2) Hosts, setting agendas, and attending a semiannual review during which the status of all major instrumentation, targets and threat projects under PM ITTS and under ATEC execution will be reviewed.

(3) Presents the authenticated prioritized listing of ITTS programs to TEMA as a coordinated agreement.

Z–14. Validation of threat simulators/simulations role

a. DUSA (OR) provides overall DA-level program direction, guidance, review, and approval authority.

b. TEMA—

(1) Approves and transmits copies of VRs with appropriate forwarding or notification letters to the DOT&E as required.

(2) When required, coordinates Air Force and Navy participation in the validation process.

(3) Prioritizes and coordinates all Army requests for threat data in support of validation.

(4) Chairs all DA level VWGs. Charters all other VWGs as warranted and appoints the chairperson.

c. TRADOC—

(1) Identifies and documents threat simulator and target requirements to support combat development efforts.

(2) Participates in VWGs as required.

d. PEO STRI—

(1) Identifies and documents threat simulator and target requirements to support testing and simulator materiel developmental efforts.

(2) Participates in VWGs as required.

e. ATEC—

(1) Identifies, prioritizes, and documents threat simulator/simulation and target requirements to support testing.

(2) Participates in VWGs and validation planning meetings as required and formally disseminates information identified in paragraph Z–14*a*.

(3) Participates in PEO STRI meetings as warranted.

f. IPCs (as appropriate for the system being validated; coordination with Air Force or Navy channels will be accomplished as required)—

(1) Prepares TSPs as tasked by DIA, and provides them to the threat system MATDEV.

(2) Participates in VWGs.

(3) In coordination with the simulator or target MATDEV, develops a set of validation criteria.

(4) Provides exploitation baseline data for actual threat systems.

g. PM ITTS—

(1) Maintains an information and suspense file on all validation activities assigned by TEMA.

(2) Notifies TEMA when DSR, IOC, and Operational validations are due so that VWGs can be established.

(3) Develops, in coordination with the appropriate IPC, a proposed set of validation criteria.

(4) Participates in VWGs as required. Chairs the validation planning meetings. In this forum or through independent review, ensures VR soundness and compliance with overall intent of the validation process prior to initial staffing with core VWG members.

(5) Coordinates measurements of threat simulator and target parameters as required for comparison to the current DIA approved IPC estimates for the threat system.

(6) Develops a complete system description containing complete narrative, pictorial, and parametric description of simulator or target for comparison with the TSP. As required, serve as a technical consultant on VWGs.

(7) Prepares certification reports as required.

(8) Provides system description and data required for section IV and appendix A of DSR and IOC VRs.

(9) Funds validation efforts for which they are the designated MATDEV.

(10) Conducts measurements of threat simulator/simulation and target parameters required for OPN validations.

(11) Notifies TEMA when OPN validations are due so that VWGs can be established.

(12) In the absence of IOC VWG approved critical parameters, develops a proposed set of OPN validation criteria in coordination with the simulator system MATDEV and the appropriate IPC.

(13) Notifies TEMA of the need for Threat Support Packages.

(14) For owned systems undergoing OPN Validation, develops an updated system description containing complete narrative, pictorial, and parametric description of simulator for comparison with the TSP. Forwards updated system descriptions along with updated TSP data from the IPC to TEMA.

(15) Provides a system description and data required for section IV and appendix A of the OPN VR.

(16) Funds OPN validations for owned systems.

h. PEO or program manager—

(1) Identifies and documents in the development system's TEMP threat simulator and target requirements to support simulator materiel development efforts.

(2) Participates in VWGs as required.

Z–15. Accreditation of threat simulators/simulations, surrogates, actuals and targets roles

a. DCS, G–2—

(1) Maintains, reviews, and validates CIPs that affect the effectiveness, survivability, or security of U.S. systems.

(2) Designates TISOs for ACAT I, ACAT II, and other OSD T&E oversight systems.

(3) Coordinates and reviews threat support throughout the life cycle of developmental systems.

(4) Chairs TCGs for ACAT I and II programs and all programs on the OSD Oversight List in accordance with AR 381–11.

(5) Participates in T&E WIPTs, TCGs, and TAWGs as appropriate.

b. TEMA coordinates with the DCS, G–2 for the integration of Army-approved threat in test programs, including DT, OT, or FDT/E, and JT&E.

c. TRADOC—

(1) Provides COIC/additional operational issues and criteria for use by the TAWG.

(2) Provides the threat TSP.

(3) Chairs the TCG for all ACAT III programs not on the OSD Oversight List, in accordance with AR 381–11.

d. PEO STRI—

(1) Participates in T&E WIPTs, TCGs and TAWGs as required.

(2) Develops the threat TSP for DT if threat force operations are to be represented.

(3) Provides target and threat simulator technical performance data for use by the TAWG in assessing threat simulator and target suitability and adequacy.

(4) Measures threat simulators as required to ensure availability and accuracy of system data for accreditation.

e. ATEC—

(1) Coordinates test planning with the appropriate threat approval authority (see AR 381–11) to define the conditions and environment of both DT and OT to ensure that an appropriate battlefield environment will be portrayed.

(2) Participates in T&E WIPTs, TCGs, and chairs TAWGs for both DT and OT.

(3) Provides test concept and test design to the TCG and TAWG for their use in assessing threat simulator and target suitability and adequacy.

(4) For owned systems, provide target and threat simulator/simulation technical and performance data for use by the TAWG in assessing threat simulator and target suitability and adequacy.

f. PM ITTS or MATDEV—

(1) Provides the current VR for use by the TAWG in assessing threat simulator/simulation and target suitability and adequacy.

(2) For systems in development, provides target and threat simulator/simulation technical and performance data for use by the TAWG in assessing threat simulator/simulation and target suitability and adequacy.

(3) Measures threat simulator/simulation and target parameters as required for systems in development to ensure availability and accuracy of data for accreditation.

(4) Participates in TAWGs.

g. IPC (as appropriate for the threat systems undergoing accreditation)—

(1) Participates in T&E IPT WIPT, TCGs, and TAWGs are required to explain threat capabilities and limitations. The IPC representative should be an expert on the threat system being simulated.

(2) Participates in the TAWG to refine threat simulator/simulation/target requirements and assess the impacts of difference between the simulator/simulation/target and the threat.

(3) Provides threat assessments and documentation to the TAWG.

(4) Updates or verifies threat data as required.

h. PEO or program manager (as appropriate for weapon system undergoing test)—

(1) Establishes TAWGs under the auspices of the T&E WIPT.

(2) Participates in TAWGs as appropriate.

(3) Requests waivers for systems that have not undergone validation.

Glossary

Section I

Abbreviations

AMC
U.S. Army Materiel Command

AMCOM
U.S. Army Aviation and Missile Command

AMSAA
Army Materiel Systems Analysis Agency

AR
Army regulation

CCB
configuration control board

CE
continuous evaluation

CG
commanding general

CPU
central processing unit

CSA
Chief of Staff, U.S. Army

DA
Department of the Army

DA Pam
Department of the Army pamphlet

DAT
damage assessment team

DCS
Deputy Chief of Staff

DIA
Defense Intelligence Agency

DoD
Department of Defense

DoDD
Department of Defense directive

DoDI
Department of Defense instruction

DPG
U.S. Army Dugway Proving Ground

DT&E
development test and evaluation

DTP
detailed test plan

ECP
engineering change proposal

ECP–S
engineering change proposal-software

EIS
environmental impact statement

EMP
electromagnetic pulse

EW
electronic warfare

FAR
Federal Acquisition Regulation

FM
field manual

FYTP
Five-Year Test Program

HFE
human factors engineering

HQDA
Headquarters, Department of the Army

IAW
in accordance with

IC
integrated concept

ICT
integrated concept team

IER
information exchange requirement

IIPT
integrating integrated product team

ILS
integrated logistics support

IOC
initial operational capability

IOT&E
initial operational test and evaluation

JMEM
Joint Munitions Effectiveness Manual

MACOM
major Army command

MIL–HDBK
military handbook

MIL–STD
military standard

MOE
measure of effectiveness

MOP
measure of performance

MOPP
mission-oriented protection posture

MTBF
mean-time-between-failure

MTMC
Military Traffic Management Command

NATO
North Atlantic Treaty Organization

NBC
nuclear, biological, chemical

NET
new equipment training

OSD
Office of the Secretary of Defense

OT
operational testing

PA
pattern of analysis

PIP
product improvement program

PM
program, project, and product manager

POI
program of instruction

POM
program objective memorandum

RDT&E
research, development, test, and evaluation

RF
radiofrequency

RFP
request for proposal

SED
Software Engineering Directorate

SMDC
U.S. Army Space and Missile Defense Command

SOW
statement of work

TIR
test incident report

TM
technical manual

TMDE
test, measurement, and diagnostic equipment

TRADOC
U.S. Army Training and Doctrine Command

TSARC
test schedule and review committee

USAKA
U.S. Army Kwajalein Atoll

USC
United States Code

WBS
work breakdown structure

WSMR
U.S. Army White Sands Missile Range

YPG
U.S. Army Yuma Proving Ground

Section II

Terms

Accreditation
The official determination that a model, simulation, or federation of M&S is acceptable for use for a specific purpose. Accreditation for threat simulators/simulations, surrogates, actual threat systems, and targets is the process used to determine whether threat simulators/simulations, surrogates, actual threat systems, and targets are suitable for a specific test.

Acquisition
The process consisting of planning, designing, producing, and distributing a weapon system/equipment.

Acquisition category
ACAT I programs are those programs that are MDAPs or that are designated ACAT I by the MDA as a result of the MDA's special interest. In some cases, an ACAT IA program, as defined below, also meets the definition of a MDAP. The USD (AT&L) and the ASD (C3I)/DoD CIO will decide who will be the MDA for such AIS programs. Regardless of who is the MDA, the statutory requirements that apply to MDAPs will apply to such AIS programs. ACAT I programs have two sub-categories: ACAT ID, for which the MDA is USD (AT&L) (the "D" refers to the Defense Acquisition Board (DAB), which advises the USD (AT&L) at major decision points) or ACAT IC, for which the MDA is the DoD Component Head or, if delegated, the DoD Component Acquisition Executive (CAE). ACAT IA programs are those programs that are MAISs or that are designated as ACAT IA by the MDA as a result of the MDA's special interest. ACAT IA programs have two sub-categories: ACAT IAM for which the MDA is the CIO of the DoD, the ASD (C3I) (the "M" (in ACAT IAM) refers to MAIS) or ACAT IAC, for which the DoD CIO has delegated MDA to the CAE or Component CIO (the "C" (in ACAT IAC) refers to component). The ASD (C3I) designates programs as ACAT IAM or ACAT IAC. ACAT II programs are those programs that do not meet the criteria for an ACAT I program, but that are Major Systems or that are designated as ACAT II by the MDA as a result of the MDA's special interest. Because of the dollar values of MAISs, no AIS programs are ACAT II. The MDA is the CAE or the individual designated by the CAE. ACAT III programs are defined as those acquisition programs that do not meet the criteria for an ACAT I, an ACAT IA, or an ACAT II. The MDA is designated by the CAE and will be at the lowest appropriate level. This category includes less-than-major AISs.

Advanced concept technology demonstration
A user-oriented and dominated demonstration and/or experiment, and evaluation. It provides a mechanism for intense involvement of the warfighter while incorporation of technology into a warfighting system is still at the informal stage. Technology demonstrations are selected based on recommendations to OSD that are nominated by CG, TRADOC and approved for transmittal to OSD by ASA (ALT) and DCS for Operations and Plans for participation in the ACTD program. There are three driving motivations: gain understanding of military utility before committing to large-scale acquisition; develop the corresponding concepts of operation and doctrine to make the best use of the new capabilities; and provide limited, initial residual capabilities to the forces for up to 2 years. OSD partially funds the selected ACTDs. (See DA Pam 70–3.)

Advanced technology demonstration
A pre-acquisition mechanism for the warfighter to explore military utility and potential of technologies to support warfighting concepts. This is a pre-acquisition mechanism for the warfighter to explore the technical feasibility, affordability, and potential of technologies to support warfighting concepts. A successful ATD will allow accelerated entry into the acquisition life cycle (such as at milestone B or C). ATDs are relatively large scale in resources and complexity, but typically focus on an individual system or subsystem. The user is involved throughout the process. Experimentation is with Soldiers in a real or synthetic environment. It has a finite schedule of 5 years or less with exit criteria established by the MATDEV and TRADOC. (See DA Pam 70–3.)

Advanced warfighting experiment
Culminating efforts in the process to evaluate major increases in warfighting capability. They cross DOTMLPF domains and synergistically combine new force structure, doctrine, and materiel to counter a tactically competent opposing force. Moreover, they impact most, if not all, battlefield dynamics and battlefield operating systems. These experiments use progressive and iterative mixes of high-fidelity constructive, virtual, and live simulation to provide the Army leadership with future operational capability insights. AWEs are sponsored by the CG, TRADOC and approved and resourced by the CSA.

Allocated baseline
The initially approved documentation describing an item's functional, interoperability, and interface characteristics that are allocated from those of a system or a higher level CI, interface requirements, with interfacing CIs, additional design constraints, and the verification required to demonstrate the achievement of those specified characteristics.

Analysis of alternatives
The AoA is a rigorous, quantitative analysis, conducted by TRADOC, designed to assess multiple program alternatives along the lines of cost, operational effectiveness, and technical risk as well as the tradeoffs between these elements. The findings from the AoA provide the analytic underpinnings for development of the ORD and refinements to the ORD KPPs. A list of supporting analyses, including AoA results, is attached to the ORD. This list includes a short description summary of the analyses used to develop the ORD and a synopsis of key pertinent results.

Automated information system
A combination of information, computer and telecommunications resources and other IT and personnel resources that collects, records, processes, stores, communicates, retrieves, and displays information (see AR 25–3).

Availability
Measure of the degree to which an item is in an operable and committable state at the start of a mission, when the mission is called at an unknown (random) point in time.

Ballistic hull and turret
An armored structure representative of a system without powerpack or component sub-systems.

Baseline
Configuration documentation formally designated and fixed at a specific time during a CI's life cycle. Configuration baselines, plus approved changes from those baselines constitute the current configuration.

Battle labs
Organizations chartered by the CG, TRADOC with the mission to plan, conduct, and report warfighting experiments supporting the requirements determination process. Battle Labs provide linkage with the scientific and technical and acquisition communities on ACTDs, ATDs, and Advanced Concepts in Technology Program II (ACT II) demonstrations and provide for participation in technology reviews (AR 71–9).

Benchmark Test Files
A database of known content against which a controlled set of inputs is processed and from which output results may be predicted. This term is used in reference to a test environment and pre-established test cases/data.

Board of Directors for test and evaluation
The Executive Agent for the oversight of the T&E infrastructure. The Board of Directors (Board of Directors) has authority over the Services relating to their T&E infrastructure investment, infrastructure consolidation, standards, and policy relating thereto. The Board of Directors ensures that modernization investments are made at test facilities and ranges that are best suited to support required testing without regard to Service ownership. The Board of Directors also ensures that the Services develop streamlining, consolidation, and downsizing initiatives for the T&E Infrastructure. The Board of Directors is composed of the Vice-Chiefs of the three Services, supported by the Service T&E Principals (DUSA (OR), N–091, and AF/TE). The Assistant Commandant Marine Corps is an advisory member. The

Joint Staff participates as a member for advocacy of subjects of their interest (for example, training, and so forth). The Board of Directors also establishes liaison and coordinates plans, as deemed necessary, with the Joint Chiefs of Staff, DoD Agencies, OSD, and cognizant Unified and Specified Commands.

Board of Directors, Executive Secretariat
The Board of Directors, Executive Secretariat will lead development of corporate guidance for T&E infrastructure management, standards and policy, configuration, and investments. The Board of Directors, Executive Secretariat will lead the implementation of T&E reliance. The Board of Directors, Executive Secretariat is composed of the T&E Principals (DUSA (OR), Air Force Test and Evaluation, Navy Test and Evaluation, and the DOT&E Rescues and Ranges). The Board of Directors, Executive Secretariat is chaired by the T&E Principal from the organization of the chair of the Board of Directors, on the same 2-year rotational basis.

Brassboard configuration
An experimental device (or group of devices) used to determine feasibility and to develop technical and operational data. It will normally be a model sufficiently hardened for use outside of laboratory environments to demonstrate the technical and operational principles of immediate interest. It may resemble the end-item but is not intended for use as the end-item.

Breadboard configuration
An experimental device or group of devices used to determine feasibility and to develop technical data. It will normally be configured only for laboratory use to demonstrate the technical principles of immediate interest. It may not resemble the end-item and is not intended for use as the projected end-item.

Building-block approach
An approach to vulnerability/lethality testing beginning with component level testing and progressing through subsystem, system, ballistic hull and turrets testing, and culminating in a full-up, system-level LFT.

Catastrophic kill
An armored vehicle sustains a K-kill when both a M-kill and a F-kill occur and it is not economically repairable.

Code walkthrough
The process of assessing the level of software performance and design structure that requires the developer to demonstrate the capabilities of the software to technical, functional, and user representatives.

Combat developer
A command, agency, organization, or individual that commands, directs, manages, or accomplishes the combat developments work. Combat developments is the process of—
a. Analyzing, determining, documenting, and obtaining approval of warfighting concepts, future operational capabilities, organizational requirements and objectives, and materiel requirements.
b. Leading the Army community in determining solutions for needed future operational capabilities that foster development of requirements in all DOTMLPF domains.
c. Providing user considerations to, and influence on, the Army's scientific and technical program.
d. Integrating the efforts and representing the user across the DOTMLPF domain during the acquisition of materiel and development of organizational products to fill those requirements.

Combined developmental test and operational test
A single event that produces data to answer developmental and operational system issues. A Combined DT/OT is usually conducted as a series of distinct DT and OT phases at a single location using the same test items. For the case where a single phase can be used to simultaneously meet developmental and operational issues, this testing will be referred to as an Integrated DT/OT. Combined DT/OT and Integrated DT/OT are encouraged to achieve time, cost, and resource savings. However, they should not compromise DT and OT objectives in accordance with the Defense Acquisition Guidebook.

Command, control, communication, and intelligence interoperability recertification test
A test conducted for C4I systems if major hardware and software modifications to the C4I system have been made that impact on previously established joint interface requirements.

Command, Control, Communications, and Computer System
Integrated systems of doctrine, procedures, organizational structures, personnel, equipment, facilities, and communications designed to support a commander's exercise of command and control across the range of military operations.

Command, control, communications, computers, and intelligence interoperability certification test
A test that applies to C4I systems that has interfaces or interoperability requirements with other systems. This test may consist of simple demonstrations using message analysis or parsing software with limited interface connectivity, or extend to full-scale scenario-driven exercises with all interfaces connected.

Commercial item
An item available in the commercial marketplace that requires only modifications of a type customarily available in the commercial marketplace or minor DoD-unique modifications is considered a commercial item. The item does not have to be "off-the-shelf" to be classified as a commercial item. Two types of modifications are available: modifications of a type available in the commercial marketplace; and minor modifications of a type not customarily available in the commercial marketplace, made to DoD requirements. For modifications of a type available in the commercial marketplace, the size or extent of the modifications is unimportant. For minor modifications, the item needs to retain a predominance of non-governmental functions or essential physical characteristics. In either case, the source of funding for the modification does not impact its qualification as a commercial item.

Compartment model
A low resolution vulnerability/lethality assessment computer model used to predict the vulnerability of armored vehicles and the lethality of anti-armor munitions (see fig 5–2).

computer aided software engineering tools
Computer aided software engineering (CASE) tools are systems for building systems; they automate elements of the requirements analysis, design, development or test process.

Computer resource life cycle management plan
The primary Government planning document to be used at all decision levels for assessing the adequacy of the overall computer resources management efforts throughout a system's life (see DoDI 5000.02).

Computer resources
The totality of computer personnel, documentation, services, and supplies applied to a given effort. This includes hardware, software, services, personnel, documentation and supplies.

Computer resources work group
Established by the MATDEV after Milestone B for each AR 70–1 system to aid in the management of system computer resources. The computer resources work group assists in insuring compliance with policy, procedures, plans and standards established for computer resources (see AR 73–1).

Computer software configuration item
A CI that is software.

Concept experimentation program
A separately funded TRADOC warfighting experimentation program supporting the DOTMLPF operational requirements determination sponsors (TRADOC centers and schools, Army Medical Department Center and School, and SMDC CBTDEVs) and the ability to investigate military utility of and capitalize on technologies, materiel, and warfighting ideas. The CEP provides funding and other resources to conduct warfighting experimentation supporting the Army Experimentation Campaign Plan to provide insights to support refinement of warfighting concepts, determination of DOTMLPF needs solution to approved future operational capabilities, development of materiel requirements, and support evaluation of organizations for fielding. The CEP is an annual program that provides commanders a quick experimentation response process.

Configuration item
An aggregation of hardware, software, or both that satisfies an end use function and is designated by the Government for separate configuration management.

Configuration management
A discipline applying technical and administrative direction and surveillance to identify and document the functional and physical characteristics of a CI, control changes to those characteristics, and record and report change processing and implementation status.

Continuous evaluation
A process that provides a continuous flow of T&E information on system status and will be employed on all acquisition programs. It is a strategy that ensures responsible, timely, and effective assessments of the status of a system.

Conventional weapon
Those weapons that are neither nuclear, chemical, or biological.

Covered product improvement program
A covered system and/or major munition or missile program for which a planned modification or upgrade is likely to produce a significant effect on the vulnerability and/or lethality of that system/munition or missile.

Covered system
Any vehicle, weapon platform, or conventional weapon system that includes features designed to provide some degree of protection to users in combat and is a major system.

Criteria (for critical operational issues and criteria)
Those MOPs that, when achieved, signify that the issue has been satisfied for the supported milestone decision.

Critical operational issues
Those key operational concerns, expressed as questions that, when answered completely and affirmatively signify that a system or materiel change is operationally ready to transition to FRP.

Critical operational issues and criteria
Key operational concerns (that is, the issues) of the decision maker, with bottom line standards of performance (that is, the criteria) that, if satisfied, signify the system is operationally ready to proceed beyond the FRP DR. The COIC are not pass/fail absolutes but are showstoppers such that a system falling short of the criteria should not proceed beyond the FRP unless convincing evidence of its operational effectiveness, suitability, and survivability is provided to the decision makers/authorities. COIC are few in number, reflecting total operational system concern and employing higher order measures.

Customer test
A test conducted by a test organization for a requesting agency external to the test organization. The requesting agency coordinates support requirements and provides funds and guidance for the test. It is not directly responsive to Army program objectives and is not scheduled or approved by the TSARC unless external operational sources are required for test support.

Cycle/system test
The final phase of developer information systems testing that involves the testing of modules/programs/cycles that are integrated into the total system.

Depot level support
The level of repair performed by depot mechanics with depot tools and procedures.

Detailed test plan
This plan is used to supplement the EDP with information required for day-to-day conduct of the test. It provides requirements for activities to be conducted to ensure proper execution of the test. The DTP is a document compiled by the activity responsible for test execution.

Developer tests
Testing, modeling, and experimentation conducted by the system developer. Formal tests normally involve system level integration and certification by the developer with formal Government monitoring. Informal tests involve lower level code and unit development with internal integration between system elements. Experimentation includes a wide variety of tests, models, development techniques and simulations used to validate design concepts and theories.

Development tools
Products that are necessary to prepare, test and evaluate software units currently under development.

Developmental test readiness review
A review conducted by the program manager to determine if the materiel system is ready for the PQT or the IT is ready for the SQT.

Developmental test readiness statement
A written statement prepared by the chairperson of the DTRR as part of the minutes. The statement documents that the materiel system is ready for the PQT or the IT is ready for the SQT.

Developmental test/testing
Any engineering-type test used to verify the status of technical progress, verify that design risks are minimized, substantiate achievement of contract technical performance, and certify readiness for IOT. The DTs generally require instrumentation and measurements and are accomplished by engineers, technicians, or Soldier user test personnel.

Developmental tester
The command or agency that plans, conducts, and reports the results of Army DT. Associated contractors may perform technical testing on behalf of the command or agency.

Doctrine
The fundamental principles by which the military force or elements guide their actions to support national objectives.

Doctrine and organization test support package
A set of documentation prepared or revised by the CBTDEV or FP for each OT supporting a milestone decision. Major components of the D&O TSP are means of employment, organization, logistics concepts, OMS/MP, and test setting.

Doctrine developer
Command, agency, organization, or individual that commands, directs, manages, or accomplishes doctrine development work. Doctrine developments is the process of researching, conceptualizing, analyzing, integrating, determining, documenting, publishing, distributing, and articulating requirements for and products (for example, FMs) of doctrine and TTP.

Driver
Software that controls a hardware device or the execution of other programs.

Dynamic analysis
A test method that involves executing or simulating a product under development. Errors are detected by analyzing the response of the product to sets of input data.

Early user test
A generic term, encompassing all system tests employing representative user troops during the technology development phase or early in system development and demonstration phase. The EUT may test a materiel concept, support planning for training and logistics, identify interoperability problems, and/or identify future testing requirements. EUT provides data for the SER in support of MS B. FDT/E or CEP or both may comprise all or part of EUT. An EUT is conducted with RDT&E funds. The EUT uses procedures that are described for IOTs, modified as necessary by maturity or availability of test systems and support packages. The EUTs seek answers to known issues that must be addressed in the SER.

Electromagnetic environmental effects
Describes the impact of the electromagnetic environment on the operational capability of military forces, equipment, systems, and platforms. These effects encompass all electromagnetic disciplines, including EMC; EMI; EMV; EMP; electronic counter-countermeasures; hazards of electromagnetic radiation to personnel, ordnance, and volatile materials; and natural phenomena effects of lightning, electrostatic discharge, and p-static.

Emulation
An interpretation similar to simulation, however, the interpretation is done through hardware or microcode or the process of using software or peripherals to make one set of hardware operate like another.

Engineering change proposal—software
A term that includes both a proposed engineering change and the documentation by which the change is described and suggested (see AR 25–1).

Engineering development test
A DT conducted during system development and demonstration to provide data on performance, safety, NBC survivability, achievement of a system's CTPs, refinement and ruggedization of hardware configurations, and determination of technical risks. An EDT is performed on components, subsystems, materiel improvement, commercial items and NDI, hardware-software integration, and related software. EDT includes the testing of compatibility and interoperability with existing or planned equipment and systems and the system effects caused by natural and induced environmental conditions during the development phases of the materiel acquisition process.

Entrance criteria
Parameters that must be achieved before entry into a specific event is allowed.

Evaluation
Evaluation is an independent process by the independent evaluators to determine if a system satisfies the approved requirements. This evaluation is independent of the MATDEVs evaluation to ensure objectivity. The evaluation will assess data from all credible sources. Some data sources are simulation, modeling, and an engineering or operational analysis to evaluate the adequacy and capability of the system.

Evaluator
An individual in a command or agency, independent of the MATDEV and the user, that conducts overall evaluations of a system's operational effectiveness, suitability, and survivability.

Event design plan
Contains detailed information on event design, methodology, scenarios, instrumentation, simulation and stimulation, data management, and all other requirements necessary to support the evaluation requirements stated in the SEP.

Exit criteria
Critical, program specific results that must be attained during the next acquisition phase, as documented in the Acquisition Decision Memorandum. Exit criteria can be viewed as gates through which a program must pass during that phase. They can include, for example, the requirement to achieve a specified level of performance in testing, or conduct of a critical design review prior to committing funds for long lead item procurement, or demonstration of the adequacy of a new manufacturing process prior to entry into LRIP. Performance exit criteria are measures of technical and/or operational performance identified as exit criteria for a system.

Firepower kill
An armored vehicle suffers a F-kill if it becomes incapable of delivering accurate, controlled firepower and cannot be repaired by the crew (within approximately 10 minutes) on the battlefield.

Firmware
A combination of hardware device and computer instructions or computer data that reside as read-only software on the hardware device. The software cannot be readily modified under program control.

First article test
Conducted for quality-assurance purposes to qualify a new manufacturer or procurements from previous source out of production for an extended period (usually 2 years) and to produce assemblies, components, or repair parts conforming to requirements of the technical data package. FATs may be conducted at Government facilities or at contractor facilities when observed by the Government.

Five Year Test Program
A compendium of TSARC-recommended and DCS, G–3-approved OTPs in the following 5 years. The FYTP identifies validated requirements to support the Army's user test programs. It is developed within the existing budget and program constraints in accordance with Army priorities. It is a tasking document for the current and budget years and provides test planning guidelines for the subsequent years.

Follow-on operational test
A test conducted during and after the production phase to verify correction of deficiencies observed in earlier tests, to refine information obtained during IOT; to provide data to evaluate changes; or to provide data to re-evaluate the system to ensure that it continues to meet operational needs.

Force development test or experimentation
A TRADOC-funded test and experimentation program supporting force development processes by examining the effectiveness of existing or proposed concepts or products of DOTLPF. In addition to supporting stand-alone DOTLPF efforts, FDT/E may be conducted as needed during acquisition to support development and verification of system DOTLPF.

Foreign comparative testing
The T&E of NATO and non-NATO allies' defense equipment to determine whether such equipment meets valid existing DoD needs. The FCT Program's primary objective is to leverage NDI of allied and friendly nations to satisfy DoD requirements or correct mission area shortcomings.

Full-up testing
Firings against full-scale targets containing all of the dangerous materials (for example, ammunition, fuel, hydraulic fluids, and so forth), system parts (for example, electrical lines with operating voltages and currents applied, hydraulic lines containing appropriate fluids at operating pressures, and so forth), and stowage items normally found on that

target when operating in combat. Full-up testing includes firings against full-up components, full-up sub-systems, full-up sub-assemblies, or full-up systems. The term "full-up, system-level testing" is synonymous with "realistic survivability testing" or "realistic lethality testing" as defined in the legislation covering LFT.

Functional baseline
The initially approved documentation describing a system's or item's functional, interoperability, and interface characteristics and the verification required to demonstrate the achievement of those specified characteristics.

Functional configuration audit
A formal examination of the functional characteristics of a CI, prior to acceptance, to verify that the item has achieved the requirements specified in its functional and allocated configuration documentation.

Functional proponent
A command, Army staff element, or agency that accomplishes the function of CBTDEV, TNGDEV, trainer, and doctrine developer for IT.

Hardware configuration Item
A CI that is hardware.

Implementation procedures
A document that provides information to users and data processing personnel to install the AIS and achieve operational status.

Independent safety assessment
A document prepared by the United States Army Safety Center and forwarded to the AAE assessing the risk of the residual hazards in a system prior to the milestone DRs.

Independent verification and validation
Systematic evaluation performed by an agency that is not responsible for developing the product or performing the activity being evaluated.

Information exchange requirements
IERs characterize the information exchanges to be performed by the proposed family-of-systems, system-of-systems, or system. For ORDs, top-level IERs are defined as those information exchanges that are external to the system (that is, with other C/S/A, allied and coalition systems). IERs identify who exchanges what information with whom, why the information is necessary, and how the information exchange must occur. Top-level IERs identify warfighter information used in support of a particular mission-related task and exchanged between at least two operational systems supporting a joint or combined mission. The quality (that is, frequency, timeliness, security) and quantity (that is, volume, speed, and type of information such as data, voice, and video) are attributes of the information exchange included in the IER.

Information technology system
Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. Also includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.

Initial operational test
The dedicated field test, under realistic combat conditions, of production or production-representative items of weapons, equipment, or munitions to determine operational effectiveness, suitability, and survivability for use by representative military or civilian users.

Instrumentation
As electromagnetic (for example, electrical, electronic, laser, radar, and photosensitive) and other equipment (for example, optical, electro-optical, audio, mechanical, and automated information) is used to detect, measure, record, telemeter, process, or analyze physical parameters or quantities encountered in the T&E process. Instrumentation may apply to a system under test or to a target or threat simulator.
a. Major instrumentation.
Instrumentation that satisfies joint Service requirements, serves multiple Army commands, requires a significant level or development and integration, or has a large dollar value. Major Army instrumentation acquisition is normally PM-managed.
b. Sustaining instrumentation.

Instrumentation that is not defined a major and that satisfies within a single command, routine or recurring needs and normally acquired by the requiring command.

Integrated concept team
A multidisciplinary team used by TRADOC and other CBTDEVs to develop and coordinate warfighting concepts, to determine and coordinate DOTMLPF needs to fulfill future operational capabilities, and to develop and coordinate potential materiel requirements when applicable.

Integrated developmental testing/operational testing
Integrated DT/OT, a special case of a combined DT/OT, is a single phased event that generates data to address developmental and operational issues simultaneously under operational conditions. The execution strategy for this event is based on the requirements of the program.

Integrated product and process development
IPPD is a technique that integrates all acquisition activities in order to optimize system development, production, and deployment. Key to the success of the IPPD concept are the IPTs, which are composed of qualified and empowered representatives from all appropriate functional disciplines who work together to identify and resolve issues. As such, IPTs are the foundation for organizing for risk management.

Integrated product and process management
A management process that integrates all activities from product concept through production and field support, using a multifunctional team, to simultaneously optimize the product and its manufacturing and sustainment processes to meet cost and performance objectives.

Integrated product team
A team composed of representatives from all appropriate functional disciplines and levels of organization working together with a leader to build successful and balanced programs, identify and resolve issues, and make sound and timely decisions.

Integrated testing and evaluation
A T&E strategy that reduces the multiple and redundant products and processes, and encompasses the development of a single integrated system evaluation plan and a single integrated test/simulation strategy, leading to a single SER for the customer. The process also increases the use of contractor data for evaluation and expands the use of M&S with the goal of reducing T&E costs. Integrated T&E strategies may include combined DT/OT events where appropriate.

Interface
In software development, a relationship among two or more entities (such as CSCI–CSCI, CSCI– hardware CI, CSCI-user, or software unit-software unit) in which the entities share, provide, or exchange data.

Interim change package
A software modification release of an ECP–S that, because of urgency, regulatory requirement or special need, must be provided before the availability of the next scheduled Software Change Package.

Interoperability
Ability of systems, units, or forces to provide services and to accept services from other systems, units, or forces and to use the services so exchanged to enable them to operate effectively together. Alternately, the condition achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users.

Key performance parameter
Those capabilities or characteristics considered essential for successful mission accomplishment. Failure to meet an ORD KPP threshold can be cause for the concept or system selection to be reevaluated or the program to be reassessed or terminated. Failure to meet a CRD KPP threshold can be cause for the family-of-systems or system-of-systems concept to be reassessed or the contributions of the individual systems to be reassessed. KPPs are validated by the JROC. ORD KPPs are included in the APB.

Left-of-baseline
The manual and automated processes of extracting selected data and reducing them to input file and transaction formats acceptable for building or initializing a database for a new system. Normally associated with conversion requirements or parallel testing.

Lethality
The ability of a munition (or laser, high power microwave, and so forth) to cause damage that will cause the loss or degradation in the ability of a target system to complete its designated missions.

Limited user test
Any type of RDT&E funded user test conducted that does not address all of the effectiveness, suitability, and survivability issues and is therefore limited in comparison to an IOT that must address all effectiveness, suitability, and survivability issues. The LUT addresses a limited number of operational issues. The LUT may be conducted to provide a data source for SAs in support of the LRIP decision (MS C) and for reviews conducted before IOT. The LUT may be conducted to verify fixes to problems discovered in IOT that must be verified prior to fielding when the fixes are of such importance that verification cannot be deferred to the FOT.

Live fire test
A test event within an overall LFT&E strategy that involves the firing of actual munitions at target components, target sub-systems, target sub-assemblies, and/or sub-scale or full-scale targets to examine personnel casualty, vulnerability, and/or lethality issues.

Logistic demonstration
A demonstration that evaluates the achievement of maintainability goals, the adequacy and sustainability of tools, test equipment, selected test programs sets, built-in test equipment, associated support items of equipment, technical publications, maintenance instructions, trouble-shooting procedures, and personnel skill requirements. Also evaluated are the selection and allocation of spare parts, tools, test equipment, and tasks to appropriate maintenance levels, and the adequacy of maintenance time standards.

Logistician
An Army staff element that conducts or oversees the logistic evaluation of systems being acquired and assures that logistics is adequately addressed in the TEMP and DTPs.

Logistics supportability
The ability to sustain a system's required level of performance and readiness in a combat environment in accordance with approved concepts, doctrine, materiel, and personnel.

Low-rate initial production
Specified quantities of new weapon systems that provide production configured or representative articles for operational test pursuant to 10 USC 4171, establish an initial production base for the system, and permit an orderly increase in the production rate for the system sufficient to lead to FRP upon the successful completion of OT. LRIP also serves to reduce the Government's exposure to (risk of) large retrofit programs and costs subsequent to FRP and deployment.

Maintainability
Ability of an item to be retained in or restored to a specified condition when maintenance is performed by personnel having specified skill levels and using prescribed procedures and resources at each prescribed level of maintenance and repair.

Major munitions program
A conventional munitions program that is a major system within the definition given below or for which more than one million rounds are planned to be acquired.

Major system
A combination of elements that will function together to produce the capabilities required to fulfill a mission need. The elements may include hardware, equipment, software, or any combination thereof, but excludes construction or other improvements to real property. A system will be considered a major system if—
a. The DoD is responsible for the system and the total expenditures for research, development, and T&E for the system are estimated to be more than $75 million (based on fiscal year 1980 constant dollars), or the eventual total expenditure for procurement of more than $300 million (based on fiscal year 1980 constant dollars).
b. A civilian agency is responsible for the system and the total expenditures for the system are estimated to exceed $750,000 (based on fiscal year 1980 constant dollars) or the dollar threshold for a "major system" established by the agency pursuant to Office of Management and Budget, Circular A–109, whichever is greater.
c. The system is designated a major system by the Secretary of the Army.

Manpower and personnel integration
The entire process of integrating the full range of manpower, personnel, training, HFE, system safety, health hazards, and survivability throughout the materiel development and acquisition process.

Materiel developer
The research, development, and acquisition command, agency, or office assigned responsibility for the system under development or being acquired. This position can refer to the PEO, program or project manager, or others assigned to this function by the developing agency.

Materiel system computer resources
Computer resources acquired for use as integral parts of weapons; command and control; communications; intelligence and other tactical or strategic systems and their support systems. The term also includes all computer resources associated with specific program developmental T&E, OT, and PDSS, including weapon system training devices, automatic test equipment, land based test sites, and system integration and test environments.

Measure of effectiveness
A quantifiable measure used in comparing systems or concepts or estimating the contribution of a system or concept to the effectiveness of a military force. The extent to which a combat system supports a military mission.

Measure of performance
A quantifiable measure used in comparing systems or estimating the contribution of a system or concept to the effectiveness of a military force. The extent to which a combat system accomplishes a specific performance function.

Metric
A quantitative value, procedure, methodology, and/or technique that allows one the ability to measure various aspects and characteristics of software.

Milestone
A major decision point that separates discrete logical phases of an acquisition (for example, MS C (LRIP approval) determines if the results of the system development and demonstration phase warrant establishing a production baseline).

Mission effectiveness
Mission effectiveness pertains to the capability of an operational unit to carry out its critical mission tasks required to perform assigned missions, as described in the MNS and ORD. Capability is the ability of typical operators and maintainers to accomplish needed critical mission tasks.

Mission need statement
A formatted non-system specific statement containing operational capability needs and written in broad operational terms. It describes required operational capabilities and constraints to be studied during the technology development phase.

Mission suitability
Mission suitability pertains to the design characteristics needed to enable and sustain critical mission task accomplishment. Sustainability addresses the ability of the system to achieve and remain in an operable and committable state (that is, operational availability) during the course of conducting its missions.

Mission survivability
Mission survivability addresses the design characteristics needed to enable the system and operational unit to avoid, evade, and withstand the effects of the threat in order to increase mission effectiveness.

Mobility kill
An armored vehicle suffers a M-kill if it becomes incapable of executing controlled movement and cannot be repaired by the crew (within approximately ten minutes) on the battlefield.

Model/modeling
A vulnerability/lethality assessment tool used to predict one or more aspects of a given munition/target interaction. A model may be anything from a sophisticated computer code (employing many individual algorithms to assess total system vulnerability/lethality) to a simple mathematical expression or empirical relationship used to predict a single element of a munition/target interaction (for example, the penetration performance of a given munition).

New equipment training test support package
Prepared by the MATDEV in accordance with AR 350–1 to support training development for new materiel and IT, including conduct of T&E of new equipment and software. Based on the NET program, the MATDEV prepares, as appropriate, a NET TSP. The NET TSP is provided to the TNGDEVs and testers. It is used to train player personnel for DT and to conduct training of instructor and key personnel who train player personnel for OT. The TNGDEV uses the NET TSP to develop the training TSP.

Non-developmental item
Any previously developed item of supply used exclusively for governmental purposes. Item requires only minor modifications of a type customarily available in the commercial marketplace in order to meet the requirements of the DoD. Minor modification means a change that does not significantly alter the non-governmental function or essential physical characteristics of an item or component, or change the purpose of a process. Factors to be considered in determining whether a modification is minor include the value and size of the modification and the comparative value and size of the final product. Dollar values and percentages may be used as guideposts but are not conclusive evidence that a modification is minor.

Operational effectiveness
The overall degree of mission accomplishment of a system when used by representative personnel in the expected (or planned) environment. Some examples of environment are natural, electronic, threat, and so forth for operational employment of the system considering organization, doctrine, tactics, survivability, vulnerability, and threat (including countermeasures; initial NWE; nuclear, biological, and chemical contamination threats).

Operational requirements document
A formatted statement containing performance and related operational parameters for the proposed concept or system. Prepared by the user or user's representative at each acquisition milestone beginning with Milestone B.

Operational suitability
The degree to which a system can be satisfactorily placed in field use with consideration given to availability, compatibility, transportability, interoperability, reliability, wartime usage rates, maintainability, safety, human factors, manpower supportability, logistic supportability, and training requirements.

Operational survivability
The capability of a system and crew to avoid or withstand manmade hostile environments without suffering an abortive impairment of its ability to accomplish its designated mission.

Operational test readiness review
A review conducted, as deemed necessary by the operational tester, before each operational test of a system. The purpose is to identify problems that may impact on starting or adequately executing the test.

Operational test readiness statement
A written statement prepared by the CBTDEV, MATDEV, TNGDEV or trainer, and test unit commander before the start of IOTs (or FOTs) for use during the OTRR. The OTRS addresses or certifies the readiness of the system for testing in each member's area of responsibility. OTRSs may also be required for some FDT/E and should be specified in the OTP.

Operational test/testing
Any testing conducted with the production or production like system in realistic operational environments, with users that are representative of those expected to operate, maintain, and support the system when fielded or deployed.

Operational tester
The Army operational tester is a command or agency that plans, conducts, and reports the results of OT, such as ATEC, SMDC, USAMEDCOM, U.S. Army Intelligence and Security Command, or U.S. Army Corps of Engineers.

Outline test plan
An OTP is a formal resource document prepared for TSARC review. It contains resource and administrative information necessary to support an OT or FDT/E. OTPs are also prepared for DT when Soldier participants or other operational resources are required. The OTP contains the critical test issues, test conditions, scope, tactical context (OT or FDT/E only), resource requirement suspense dates, test milestone dates, and cost estimates (for user T&E only).

Overarching integrated product team
A DoD (or component-led) team usually composed of the former DAB Committee chairperson, the applicable PM and PEO, and component and OSD staff principals or their representatives. The OIPT is involved in the oversight and review of a particular ACAT 1D program. The OIPT structures and tailors functionally oriented IPTs to support the MATDEV, as needed, and in the development of strategies for acquisition/contracts, cost estimates, evaluation of alternatives, logistics management, and similar management concerns. The OIPT meets immediately after learning that a program is intended to be initiated to determine: the extent of IPT support needed for the potential program, who should participate on the IPTs, the appropriate milestone for program initiation, and the documentation needed for the program initiation review. After submission of final documentation for a milestone review, the OIPT, together

with the CAE will hold a formal meeting, chaired by the OIPT leader. This meeting will determine if any issues remain that have not been resolved earlier in the process, to assess the MATDEVs recommendations for future milestone reviews and documentation, and to determine if the program is ready to go forward for a decision. Former DAB and Service-level committees are replaced by OIPTs.

Parallel testing
Testing that demonstrates whether or not two versions of the same application are consistent, or two systems performing the same function.

Partnering
Partnering is a commitment between Government and industry to improve communications and avoid disputes. It constitutes a mutual commitment by the parties on how they will interact during the course of a contract, with the primary objective of facilitating improved contract performance through enhanced communications. It is accomplished through an informal process with the primary goal of providing American Soldiers with quality supplies and services, on time, and at a reasonable cost.

Personnel
A term used to describe the characteristics of an individual Soldier (skill/skill level).

Physical configuration audit
The formal examination of the "as-built" configuration of a CI against its technical documentation to establish or verify the CI's product baseline.

Pilot production item
An item produced from a limited production run on production tooling to demonstrate the capability to mass-produce the item.

Pk
Not a probability in the pure sense but a fractional estimate of a system's loss of function.

Pk/h
Not a probability in the pure sense but a fractional estimate of a system's loss of function given an impact on the system of interest.

Pre-production prototype
An article in final form employing standard parts and representative of articles to be produced on a production line with production tooling.

Pre-shot prediction
An a priori prediction of the expected outcomes of a live fire shot. The prediction might, in special circumstances, be a quantified value of the probability of kill given a hit and/or the expected number of casualties. Most often, the pre-shot prediction will be in the form of quantitative or qualitative expectations of the ability of the attacking munition to defeat the armor or other protective design features of the target and inflict damage to components or personnel; or conversely, the ability of the target to defeat or mitigate the effects of the attacking munition. These predictions can be either absolute expectations of performance or comparative expectations of the relative performance of two or more munitions or targets. The pre-shot predictions may be based on computer models, engineering principles, or engineering judgments.

Production prove-out test
A DT conducted before production testing with prototype hardware for the selected design alternative. The production prove-out test provides data on safety, NBC survivability, achievability of CTPs, refinement and ruggedization of hardware and software configurations, and determination of technical risks. After type classification, production prove-out testing may also be conducted to provide data that could not be obtained before type classification, such as survivability or environmental.

Production qualification test
A system-level DT conducted using LRIP assets, when available, prior to the FRP DR that ensures design integrity over the specified operational and environmental range. This test usually uses prototype or pre-production hardware fabricated to the proposed production design specifications and drawings. Such tests include contractual reliability and maintainability demonstration tests required before production release.

Production verification test
A system-level DT conducted post-FRP to verify that the production item meets CTPs and contract specifications, to determine the adequacy and timeliness of any corrective actions indicated by previous tests, and to validate the manufacturer's facilities, procedures, and processes. This test may take the form of a FAT if such testing is required in the TDP. FAT is required for quality assurance purposes to qualify a new manufacturer or procurements from a previous source out of production for an extended period and to produce assemblies, components, or repair parts satisfying the requirements of the TDP.

Program
A separately compilable, structural (closed) set of instructions most precisely associated with early generations of computers. Synonymous with computer program.

Program executive officer
The general officer or senior executive who provides the overall management of the T&E activities of assigned systems.

Program manager
A DA board selected manager (military or civilian) of a system or program. A program manager may be subordinate to the AAE, PEO, or a materiel command commander.

Proponent
For the purpose of this pamphlet, proponent refers to the TRADOC Center or School (and, to the degree it chooses to participate, the TSM) assigned lead responsibility for the system; who writes, coordinates, staffs, and prepares and presents the ORD–COIC crosswalk matrix approval briefing.

Qualification testing
Testing performed to demonstrate to the contracting agency that a CSCI or system meets its specified requirements.

Rationale (for critical operational issues and criteria)
Justification for the COI criteria and an audit trail of their link to the operational requirement (ORD/required operational capability and the AoA).

Realistic survivability testing
Testing for vulnerability and survivability of a system in combat by firing weapons likely to be encountered in combat (or munitions with a capability similar to such munitions) at the system configured for combat, with the primary emphasis on testing vulnerability with respect to potential user casualties and taking into account equal consideration for the operational requirements and combat performance of the system.

Realistic test environment
The conditions under which a system is expected to be operated and maintained, including the natural weather and climatic conditions, terrain effects, battlefield disturbances, and enemy threat conditions.

Realistic testing
For vulnerability testing: the firing of munitions, likely to be encountered in combat, at the weapon system configured for combat. For lethality testing: the firing of the munition or missile concerned at appropriate targets configured for combat.

Recovery/reconfiguration testing
Testing that verifies the recovery process and component parts' effectiveness. It validates that enough backup data are preserved and stored in a secure location.

Regression testing
Testing of a computer program and/or system to assure correct performance after changes were made to code that previously performed correctly. Includes testing or retesting those areas or aspects of a system that will or could be affected by the changes.

Release
A configuration management action whereby a particular version of software or documentation is complete and available for a specific purpose (for example, released for test).

Reliability
The duration or probability of failure free performance under stated conditions.

Reliability, availability, and maintainability
Includes the system's mission reliability, its availability in a wartime scenario, and its maintainability in the operational environment. Operational RAM includes the effects of the hardware, support equipment, personnel, manuals, and the impact of embedded software.

Requirement
A concise statement of minimum essential operational, technical, logistic, and cost information necessary to initiate full-scale development or procurement of a materiel system.

Requirements trace
Assuring requirements flow from the user specifications through design and implementation of the product.

Research effort or test
A technical effort or test conducted during pre-systems acquisition to determine early technical characteristics and to support the research of these items.

Right-of-baseline
The automated process of building a database from left-of-baseline products, or the initialization of new files introduced for the first time. Normally associated with conversion requirements or parallel testing.

Safety assessment report
A formal summary of the safety data collected during the design and development of the system. In it, the MATDEV summarizes the hazard potential of the item, provides a risk assessment, and recommends procedures or other corrective actions to reduce these hazards to an acceptable level.

Safety confirmation
A separate document that provides the MATDEV with safety findings and conclusions and states whether the specified safety requirements are met. It indicates whether the system is safe for operation or identifies hazards that are not adequately controlled or mitigated, lists any technical or operational limitations or precautions, and highlights any safety problems that require further investigation and testing.

Safety release
A formal document issued by the developmental tester to the OT organization indicating that the system is safe for use and maintenance by typical user troops and describing the specific hazards of the system based on test results, inspections, and system safety analyses.

Scope (for critical operational issues and criteria)
The operational capabilities, definitions, and conditions that focus the COI and guide its evaluation.

Simulation
The process of conducting experiments with a model for the purpose of understanding the behavior of the system. Simulations may be dynamic, engineering (scientific), environmental, instruction level, statement level, and system level. For AIS, simulation entails summary files to simulate an internal or external interface input.

Software acceptance test
A operational test of a new system or changes to a deployed system, directed by an independent tester and conducted in a field environment using a production database and executed on target hardware.

Software change package
One or more changes that have been approved and scheduled for implementation, as a group, by the appropriate CCB.

Software development
A set of activities that results in software products. Software development may include new development, modification, reuse, reengineering, maintenance, or any other activities that result in software products.

Software development file
A repository for material pertinent to the development or support of a particular body of software. Contents typically include (either directly or by reference) considerations, rationale, and constraints related to requirements analysis, design, and implementation; developer internal test information; and schedule and status information.

Software development library
A controlled collection of software, documentation, other intermediate and final software products, and associated tools and procedures used to facilitate the orderly development and subsequent support of software.

Software development test
A form of DT conducted by the software developer and the proponent agency to ensure that the technical and functional objectives of the system are met. These tests consist of program or module and cycle or system levels of testing. The unit or module test is the initial testing level. Testing is executed on local testbed hardware, and benchmark test files are used. This testing provides data to assess the effectiveness of the instruction code and economy of subroutines for efficient processing. It also ensures that input and output formats, data handling procedures, and outputs are produced correctly. The cycle or system test involves testing the combination of linkage of programs or modules into major processes.

Software engineering environment
The facilities, hardware, software, firmware, procedures, and documentation needed to perform software engineering. Elements may include, but are not limited to CASE tools, compilers, assemblers, linkers, loaders, operating systems, debuggers, simulators, emulators, documentation tools, and database management systems.

Software qualification test
A system test conducted by the developmental tester using live-data files supplemented with user prepared data and executed on target hardware. The objectives of the software qualification test are to obtain Government confirmation that the design will meet performance and operational requirements, to determine the adequacy of any corrective action indicated by previous testing, and to determine the maturity and readiness for OT.

Software test environment
The facilities, hardware, software, firmware, procedures, and documentation needed to perform qualification, and possibly other, testing of software. Elements may include but are not limited to simulators, code analyzers, test case generators, and path analyzers, and may also include elements used in the SEE.

Software transition
The set of activities that enables responsibility for software development to pass from one organization, usually the organization that performs initial software development, to another, usually the organization that will perform software support.

Software unit
An element in the design of a CSCI; for example, a major subdivision of a CSCI, a component of that subdivision, a class, object, module, function, routine, or database. Software units may occur at different levels of a hierarchy and may consist of other software units. Software units in the design may or may not have a one-to-one relationship with the code and data entities (routines, procedures, database, and data files) that implement them or with the computer files containing those entities.

Statement of work
A statement of contract requirements that is used for defining and achieving program goals. The SOW provides the basic framework for a particular effort. It is a document by which all nonspecification requirements for developer efforts must be established and defined either directly or with the use of specific cited documents.

Static analysis
A direct examination of the form and structure of a product without executing the product. It may be applied to requirements, design, or code.

Stochastic
Involving or containing random variables; the interaction between the munition and the target is stochastic.

Stress test
A test that exercises code up to, including and beyond all stated limits in order to exercise all aspects of the system (for example, to include hardware, software, and communications). Its purpose is to ensure that response times and storage capacities meet requirements.

Supplemental site test
A test that may be necessary for an IT system that executes in multiple hardware and operating system environments if there are differences between user locations that could affect performance or suitability. It supplements the IOT and UAT.

Supportability
The degree to which a system can be maintained or sustained in an operational environment.

Surveillance Tests
Destructive and nondestructive tests of materiel in the field or in storage at field, depot, or extreme environmental sites. Surveillance tests are conducted to determine suitability of fielded or stored materiel for use, evaluate the effects of environments, measure deterioration, identify failure modes, and establish or predict service and storage life. Surveillance test programs may be at the component-through-system level.

Susceptibility
The degree to which a weapon system is open to effective attack due to one or more inherent weaknesses. Susceptibility is a function of operational tactics, countermeasures, probability of enemy fielding a threat, and so forth. Susceptibility is considered a subset of survivability.

Sustaining base IT systems
These systems are used for efficiently managing Army resources, managing Army installations, and deploying and sustaining the fighting force.

System
An item or group of items that consists of materiel and/or software that, when put in the hands of users, will enable those users to accomplish assigned missions.

System analysis report
The SAR provides the detailed analyses that support a SER. It accounts for all issues and measures contained in the SEP. A SAR is also prepared to support a SA when the analysis is too detailed or inappropriate for inclusion in the SA and addresses only those issues and measures contained in the SA.

System assessment
The SA provides an assessment of the progress toward achieving system requirements and resolution of issues. The scope of issues to be addressed by the SA is flexible in that it may, or may not, cover all aspects of operational effectiveness, suitability, and survivability. It may address technical aspects of a system. For example, it may provide a program manager with an assessment of a system's exit criteria (some level of demonstrated performance) or an indication that a system is progressing satisfactorily. The SA is typically produced as input to nonmilestone decisions or inquiries and to support system evaluation.

System change
A modification or upgrade to an existing system. A modification is a change to a system that is still in production. An upgrade is a change to a system that is out of production. Such changes can be improvements to system capabilities or fixes to correct deficiencies after the FRP DR. System modifications and upgrades include multisystem changes (that is, the application of a common technology across multiple systems), increment changes, preplanned product improvements, Class I Engineering Changes, and system change package proposals.

System change package
A group of modifications documented on ECP–S that are packaged and implemented during post deployment phase.

System decision paper
The primary document used to obtain Information Technology Acquisition Board approval for IT systems. Also contains information comparable to the materiel system computer resources CRLCMP.

System evaluation
System evaluation is a process that provides a continuous flow of T&E information on system status and will be employed on all acquisition programs. It ensures responsible, timely, and effective assessments of the status of a system. System evaluation can begin as early as the battlefield functional mission area analysis for materiel systems and as early as the information management plan process for IT. It will continue through a system's post-deployment activities.

System evaluation plan
The SEP documents the evaluation strategy and overall T/SES effort of a system for the entire acquisition cycle through fielding. Integrated T&E planning is documented in a SEP. The detailed information contained in the SEP supports parallel development of the TEMP and is focused on evaluation of operational effectiveness, suitability, and survivability. While the documents are similar, the TEMP establishes what T&E will be accomplished and the SEP explains how the T&E will be performed (see chap 5).

System evaluation report
The SER provides an independent evaluation and a formal position of a system's operational effectiveness, suitability, and survivability to decision makers at milestone DRs. It addresses and answers the critical operational issues and additional evaluation focus areas in the SEP based on all available credible data and the evaluator's analytic treatment of the data.

System post-deployment review
A review conducted after deployment of the initial system to evaluate how well the operational system is satisfying user requirements.

System safety management plan
A management plan that defines the system safety program requirements of the Government. It ensures the planning, implementation, and accomplishment of system safety tasks and activities consistent with the overall program requirements.

System safety program plan
A description of planned methods to be used by the contractor to implement the tailored requirements of MIL–STD–882, including organizational responsibilities, resources, method of accomplishment, milestones, depth of effort, and integration with other program engineering and management activities and related systems.

System safety risk assessment
A document that provides a comprehensive evaluation of the safety risk being assumed for the system under consideration at the milestone DR.

System safety working group
A group, chartered by the PM, to provide program management with system safety expertise and to ensure communication among all participants.

System specification
A system level requirements specification. A system specification may be a system/subsystem specification, prime item development specification, or critical item development specification.

System support package
The SSP is a set of support elements that are used to determine the adequacy of the planned support capability. Some SSP examples are support equipment, manuals, expendable items, spares, repair parts, and tools. TMDE is also included if planned for a system in the operational (deployed) environment, provided before DT and OT, and tested and evaluated during DT and OT. The MATDEV provides the SSP. An SSP is required for all systems (materiel and information). (See AR 700–127.)

System tests
Tests that are conducted on complete hardware/software systems (including supporting elements for use in their intended environment).

Target system
Suite of hardware, or hardware and software designated as the operational configuration of the system.

Targets
Expandable devices used for tracking and/or engagement by missiles/munitions in support of T&E as well as training missions. Drone targets are air or ground vehicles converted to remote or programmable control. Ground targets are intended to represent an adversary ground vehicle system or ground based military structure. Aerial targets are intended to represent adversary aircraft and missiles. Targets may represent only selected adversary system characteristics.

Technical feasibility test
A DT conducted post milestone A to provide data to assist in determining safety, health hazards, and establishing system performance specifications and feasibility.

Technical note
A TN is used to report and preserve lessons learned, analytical techniques, methodologies, or provide supplemental data and information on technology under T&E. The target audience of Technical Notes is future testers and evaluators and other researchers but may also be used for professional, academic and technical symposia and publications.

Test and evaluation Executive Agent
Provides for oversight of the T&E infrastructure of the Services and Defense agencies. The Board of Directors is designated as the T&E Executive Agent.

Test and evaluation master plan
The TEMP is the basic planning document for a system life cycle T&E. The TEMP documents the T&E strategy and is developed and initially approved prior to program initiation. The TEMP is then updated prior to each subsequent MS and FRP DR thereafter or for a major modification. It is the reference document used by the T&E community to generate detailed T&E plans and to ascertain schedule and resource requirements associated with a given system. The TEMP describes what testing is required, who will perform the testing, what resources will be needed, and what the requirements are for evaluation.

Test and evaluation working-level integrated product team
A working group, chaired by the program manager or representative for a system, designed to optimize the use of T&E expertise, instrumentation, facilities, simulations, and models to achieve test integration, thereby reducing costs to the Army. The T&E WIPT ensures that T&E planning, execution, and reporting are directed toward common goals.

Test data report
The TDR is one of two event reports that may be used to document test results. The purpose of the TDR is to provide the detailed test description, test limitations, test team observations, and the level 3 (authenticated) test database dictionary. The TDR is normally prepared for oversight systems.

Test hooks
Software logic integrated into a system to facilitate extraction of data to support test and analysis.

Test instrumentation
Scientific or technical equipment used to measure, sense, record, transmit, and process text, or display data during materiel testing and examination. Test instrumentation is equipment that is used to create test environments representative of natural and battlefield conditions. It is also simulators or system stimulators used for measuring or depicting threat or training, teaching, and proficiency during testing; or targets used to simulate threat objects when destruction of real objects is not practical.

Test report
An event report used to document test results, whether DT or OT. For DT events, the test report is provided by the contractor or Government test agencies to the T&E WIPT members and the DR body at the conclusion of the test. For OT events, the operational test report provides the results of a test event conducted on a system or concept that includes test conditions, findings, data displays, and detailed descriptions of the data collected during the test event. For additional detail, see chapter 6.

Test resource advisory group
Implements the policies, decisions, and guidance of the T&E Executive Agent (EA), as directed by the Board of Directors, Executive Secretariat. Additionally, the Test Resource Advisory Group provides recommendations to the Board of Directors, Executive Secretariat on T&E infrastructure requirement identification and investment priorities.

Test resources
All elements necessary to plan, conduct, collect, or analyze data from a test event or program. Elements include test funding and support manpower (including travel costs), test assets (or units under test), test asset support equipment, flying hours, fuel and other expenditures. Also included are standard ammunition, technical data, simulation models, testbeds, threat simulators, surrogates and replicas, special instrumentation unique to a given test asset or test event, and targets. Also included are tracking and data acquisition instrumentation, and equipment for data reduction, communications, meteorology, utilities, photography, calibration, security, recovery, maintenance and repair, frequency management and control, and base or facility support services.

Test Schedule and Review Committee-General Officer and Working Groups
The General Officer TSARC, composed of members outlined in AR 73–1, chap 9, resolves test requirement conflicts, reviews and recommends test priorities, and recommends OTPs for inclusion in the FYTP. There are two working groups, initial and mid-cycle. The Initial Working Group meets in February and August and reviews new or revised OTPs for presentation to the General Officer TSARC for review and comment. The Mid-cycle Working Group does the same thing, meeting in April and October. Both working groups identify issues requiring General Officer TSARC resolution, and review resource allocation priorities for tests having execution and budget year requirements.

Testbeds
A system representation consisting partially of actual hardware or software or both, and partially of computer models or prototype hardware or software or both.

Threat simulator
A generic term used to describe equipment that represent adversary systems. A threat simulator has one or more characteristics that when detected by human senses or manmade sensor, provide the appearance of an actual adversary system with a prescribed degree of fidelity. Threat simulators are not normally expandable.

Threat test support package
The threat TSP is a document or set of documents that provides a description of the threat that the new system will be tested against. A threat TSP is required for all materiel systems. (See AR 381–11.)

Trainer
The agency that trains personnel to operate and maintain systems, TRADOC is the trainer for most equipment.

Training developer
Determiner and documenter of training requirements as well as the conceptualizer, developer, and executor of solutions to training requirements identified through the combat development process. The solutions may include new or revised training programs, material, methods, media, and system and non-system training devices.

Training test support package
The Training TSP consists of materials used by the TNGDEV or trainer to train test players and by the evaluator in evaluating training on a new system. This includes training of doctrine and tactics for the system and maintenance on the system. It focuses on the performance of specific individual and collective tasks during OT of a new system. The training TSP is prepared by the proponent TNGDEV and trainer and represents the individual, collective, and unit training for the system when initially fielded.

Unit testing
The lowest level developer test of software.

User acceptance test
If an operational test is required to support PDSS, then the operational tester will conduct an FOT. Otherwise the FP will conduct a UAT. The CBTDEV will conduct a UAT for systems that are required to support PDSS. For systems that have both a FP and a CBTDEV, the FP will conduct the UAT. The UAT is limited in scope relative to an FOT. The UAT's primary purpose is to verify the functionality of the changes to the non-tactical C4/IT in the user environment.

Validation
The process of determining the extent to which a M&S is an accurate representation of the real-world from the perspective of the intended use of the M&S. Validation methods include expert consensus, comparison with historical results, comparison with test data, peer review, and independent review. Validation for threat simulators/simulations and targets must not be viewed as an evaluation where the relative worth of a system is being graded; it is a process for comparing simulators/simulations and targets to DIA-approved threat data, documenting the variations, and assessing the impact of those differences on the potential use of the simulator, simulation, or target.

Verification
The process of determining that a M&S accurately represents the developer's conceptual description and specifications. Verification evaluates the extent to which the M&S has been developed using sound and established software engineering techniques.

Version
An identified and documented body of software. Modifications to a version of software (resulting in a new version) require configuration management actions by the developer, the Government or both.

Vulnerability
The characteristic of a system that causes it to suffer a definite degradation (loss or reduction of capability to perform its designated mission) as a result of having been subjected to a certain (defined) level of effects in an unnatural (manmade) hostile environment. Vulnerability is considered a subset of survivability.

Walk-through
An informal, step-by-step review of a software product during development (such as program code, test scenario, functional design) that allows feedback from other members of the development team to the creator of the particular product being reviewed.

Warfighting experimentation
A group of experiments with representative Soldiers in as realistic an operational environment as possible via application of constructive, virtual, and live simulation to produce insights supporting requirements determination. They examine: (1) Whether the warfighting concepts are achievable and effective. (2) The military utility and burdens of new and existing technologies. (3) The utility and contribution of new ideas and approaches in doctrine, TTP, training, leader developments, organization design, and Soldier specialties/abilities. Experimentation may be either a single discrete event or an iterative progressive mix of simulations as necessary to support development and/or refinement of warfighting concepts, future operational capabilities, DOTMLPF needs determination analysis report, MNS, CRDs, ORD, and so forth. Experiments are conducted by or under the oversight or assistance of one or more Battle Labs or Army proponents with warfighting requirements determination missions. Examples of warfighting experiments include AWE, CEP, ACTD, and ATD Battle Lab demonstration events.

Warfighting Rapid Acquisition Program
The WRAP is directed at accelerating procurement of systems identified through warfighting experiments as compelling successes that satisfy an urgent need. WRAPs are implemented within the existing Army structure. WRAP is compatible with and supports FAR, DoD, and Army acquisition policy (DoD 5000 series and AR 70 series). AWEs, CEPs, ATDs, ACTDs, and similar experiments where ICT, supported by a battle lab, are directly involved may be used to identify WRAP candidates. The WRAP Army Systems Acquisition Review Council, chaired by the Military Deputy AAE, meets annually to consider the approval of candidates submitted by CG, TRADOC for entry into WRAP. Congress appropriates dollars specifically to fund approved WRAP programs. Approved programs may be funded as a prototype for 2 years. Immediate funding is not guaranteed. Continued actions will be needed to obtain fully document system "Standard" type classification and full logistics support. (See AR 71–9.)

Working-level integrated product team
Composed of headquarters and component functional personnel who support the MATDEV by focusing on a particular topic such as T&E, cost analysis, performance analysis, and similar activities. An Integrating IPT will coordinate all WIPT efforts and cover all topics not otherwise assigned to another WIPT. The MATDEV or their designee will usually chair WIPTs. WIPTs provide empowered functional knowledge and experience, recommendations for program success and communicate status and unresolved issues concerning their areas of responsibility.

Section III

Special Abbreviations and Terms

Following are special abbreviations and terms encountered in the U.S. Army T&E processes and publications that are not contained in AR 25–30.

AAE
Army Acquisition Executive

ABIC
Army Battlefield Interface Concept

ABO
agents of biological origin

ACAT
acquisition category

ACTD
Advanced concept technology demonstration

ACWP
actual cost of work performed

ADCSINT
Assistant Deputy Chief of Staff for Intelligence

AEC
Army Evaluation Center

AI
additional issue

AIL
action item list

AIS
automated information system

APB
acquisition program baseline

APRF
Army Pulse Radiation Facility

APTU
Army participating test unit

APTUC
Army participating test unit coordinator

ARL
U.S. Army Research Laboratory

AROC
Army Requirements Oversight Council

ASA (ALT)
Assistant Secretary of the Army (Acquisition, Logistics and Technology)

ASD (C3I)
Assistant Secretary of Defense for Command, Control, Communications, and Intelligence

ASEC
Aerosol Simulant Exposure Chamber

ATC
U.S. Army Aberdeen Test Center

ATD
advanced technology demonstration

ATEC
U.S. Army Test and Evaluation Command

ATIRS
Army Test Incident Reporting System

ATRMP
Army Test Resources Master Plan

ATSMP
Army Threat Systems Master Plan

ATTC
U.S. Army Aviation Technical Test Center

AWE
Advanced Warfighting Experiment

BCM
baseline correlation matrix

BCWP
budgeted cost of work performed

BCWS
budgeted cost of work scheduled

BDAR
battlefield damage assessment and repair

BG
Bacillus subtilis niger var.

BLRIP
beyond low-rate initial production

BOT
Botulinum toxin

C3I
command, control, communications, and intelligence

C4/IT
command, control, communications, computers, and information technology

C4I
command, control, communications, computers, and intelligence

C4I/IT
command, control, communications, computers, and intelligence/information technology

C4ISP
command, control, communications, computers, and intelligence support plan

CA
corrective action

CAE
Component Acquisition Executive

CART
corrective action review team

CASE
computer aided software engineering

CBTDEV
combat developer

CD–ROM
compact disc read-only memory

CECOM
U.S. Army Communications-Electronics Command

CEP
concept experimentation program

CHPPM
Center for Health Promotion and Preventive Medicine

CI
configuration item

CIE
clothing and individual equipment

CIO
Chief Information Officer

CMM
capability maturity model

COIC
critical operational issues and criteria

COM
computer operation manual

COTS
commercial-off-the-shelf

CPM
computer programming manual

CRD
capstone requirements document

CRLCMP
computer resources life cycle management plan

CRTC
Cold Regions Test Center

CRU
computer resource utilization

CSCI
computer software configuration item

CTA
common table of allowances

CTP
critical technical parameter

CTSF
Central Technical Support Facility

D&O
doctrine and organization

DAB
Defense Acquisition Board

DAG
data authentication group

DD, DT&E/DS
Deputy Director, Development Test and Evaluation/Defense Systems

DISA
Defense Information Systems Agency

DITSCAP
Department of Defense Information Technology Security Certification and Accreditation Process

DOT&E
Director, Operational Test and Evaluation

DOTLPF
doctrine, organizations, training, leadership and education, personnel, and facilities

DOTMLPF
doctrine, organizations, training, materiel, leadership and education, personnel, and facilities

DR
decision review

DSM
data source matrix

DSR
design system review

DT
developmental testing

DTC
U.S. Army Developmental Test Command

DTRR
developmental test readiness review

DTRS
developmental test readiness statement

DUSA (OR)
Deputy Under Secretary of the Army (Operations Research)

E3
electromagnetic environmental effects

EDP
event design plan

EDT
engineering development test

EMC
electromagnetic compatibility

EMI
electromagnetic interference

EMV
electromagnetic vulnerability

EP
electronic protect

EPG
U.S. Army Electronic Proving Ground

ERB
emerging results brief

FACITT
Facilities and Capability Information for Test and Training

FAT
first article test

FBCB2
Force XXI Battle Command Brigade and Below

FBR
Fast Burst Reactor

FCT
foreign comparative testing

FDT/E
force development test or experimentation

FNSI
finding of no significant impact

FP
functional proponent

FRP
full-rate production

FSM
firmware support manual

FUSL
full-up, system level

FWHM
full-width at half max

FXR
flash x-ray

FY
fiscal year

GEMACS
General Electromagnetic Model for the Analysis of Complex Systems

GRF
gamma radiation facility

HEL
high-energy laser

HELSTF
High Energy Laser Systems Test Facility

HEMP
high-altitude electromagnetic pulse

HERO
hazards of electromagnetic radiation to ordnance

HHAR
health hazard assessment report

HRED
Human Research and Engineering Directorate

IA
information assurance

IEB
independent evaluation brief

IKPT
instructor and key personnel training

ILSMT
integrated logistics support management team

IMPRINT
Improved Performance Research Integration Tool

INR
initial nuclear radiation

IOT
initial operational test

IPC
intelligence production center

IPPD
integrated product and process development

IPT
integrated product team

ISO
International Standards Organization

IT
information technology

ITOP
International Test Operations Procedure

ITTS
instrumentation, targets, and threat simulators

IV&V
independent verification and validation

IWG
instrumentation working group

JARP
Joint Analysis Review Panel

JITC
Joint Interoperability Test Command

JLF
Joint live fire

JROC
Joint Requirements Oversight Council

JT&E
Joint Test and Evaluation

JTA
Joint Technical Architecture

JTF
Joint Task Force

KPA
key process area

KPP
key performance parameter

LAN
local area network

LBTS
Large Blast Thermal Simulator

LCSEC
life cycle software engineering center

LD
logistics demonstration

LFT
live fire testing

LFT&E
live fire test and evaluation

LINAC
Linear Electron Accelerator

LP
limited procurement

LRU
line replaceable unit

LSA
logistic support analysis

LSAR
logistics support analysis record

LSTF
Lothan Solomon Life Sciences Test Facility

LUT
limited user test

M&S
modeling and simulation

MAC
maintenance allocation chart

MAIS
major automated information system

MANPRINT
manpower and personnel integration

MATDEV
materiel developer

MCCR
mission critical computer resources

MDA
milestone decision authority

MDAP
major defense acquisition program

MFDC
multi functional data collector

MIRACL
Mid-Infrared Advanced Chemical Laser

MNS
mission need statement

MOS
measure of suitability

MP
mission profile

MRTFB
Major Range and Test Facility Base

MTF
Marvin Bushnell Materiel Test Facility

NBCCS
nuclear, biological, chemical contamination survivability

NIE
North Atlantic Treaty Organization Consultation, Command and Control Interoperability Environment

NIETI
North Atlantic Treaty Organization Interoperability Environment Testing Infrastructure

NIETWG
North Atlantic Treaty Organization Consultation, Command and Control Interoperability Environment Testing Working Group

NOI
notice of intent

NWE
nuclear weapons effects

OIPT
overarching integrated product team

OMS
operational mode summary

ORD
operational requirements document

OT&E
operational test and evaluation

OTA
operational test agency

OTC
U.S. Army Operational Test Command

OTICC
Office of the Secretary of Defense Test Investment Coordinating Committee

OTRR
operational test readiness review

OTRS
operational test readiness statement

OUSD (AT&L)
Office of the Under Secretary of Defense (Acquisition, Technology and Logistics)

PCR
problem change report

PDSS
post deployment software support

PEO
program executive officer

PEO STRI
Program Executive Office for Simulation, Training and Instrumentation

PM ITTS
Project Manager for Instrumentation, Targets, and Threat Simulators

POA&M
plans of action and milestones

PPBES
Planning, Programming, Budget, Execution System

PPSS
post production software support

PQT
production qualification test

PVT
production verification test

QDR
quality deficiency report

RAM
reliability, availability, and maintainability

RAS
remote access server

REBA
relativistic electron beam accelerator

RH
relative humidity

RHA
rolled homogeneous armor

RPSTL
repair parts/special tools list

RTS
U.S. Army Ronald Reagan Ballistic Missile Defense Test Site

RTTC
U.S. Army Redstone Technical Test Center

S/W
software

SA
system assessment

SAC
Senior Advisory Council

SAR
system analysis report

SCOM
software center operator manual

SCP
software change proposal

SEB
Staphylococcal Enterotoxin B

SEE
software engineering environment

SEI
Software Engineering Institute

SEP
system evaluation plan

SER
system evaluation report

SIOM
software input/output manual

SIPRNET
Secret Internet Protocol Router Network

SIPT
supportability integrated product team

SLAD
Survivability/Lethality Analysis Directorate

SLOC
source lines of code

SMMP
System manpower and personnel integration management plan

SOP
standard operating procedures

SPS
software product specification

SRS
system requirements specification

SSA
software support activity

SSP
simulation support plan

SSPCL
system support package components list

SSPP
system safety program plan

SSRA
system safety risk assessment

STA
system threat assessment

STANAG
standardization agreement

STAR
system threat assessment report

STD
software test description

STEP
simulation, test, and evaluation process

STL
Semiconductor Test Laboratory

STR
software trouble report

STRAP
system training plan

STrP
software transition plan

SUM
software user manual

SVD
software version description

T&E
test and evaluation

T/SES
test/simulation execution strategy

TASL
Thermal Analysis of Skins Under Load

TAWG
threat accreditation working group

TCG
threat coordination group

TDL
tactical data link

TDLITS
Tactical Data Link Interoperability Testing Syndicate

TDR
test data report

TEM/REV
Tem/Reverberation

TEMA
Test and Evaluation Management Agency

TEMAC
Test and Evaluation Managers Committee

TEMP
test and evaluation master plan

TEMPEST
Transient Electromagnetic Pulse Emanation Standard

TFT
technical feasibility test

TI
threat integrator

TISO
threat integration staff officer

TNGDEV
training developer

TRR
test readiness review

TRTC
Tropic Regions Test Center

TSIWG
threat simulator investment working group

TSM
U.S. Army Training and Doctrine Command system manager

TSMO
Threat Systems Management Office

TSP
test support package

TTP
tactics, techniques, and procedures

UAT
user acceptance test

UFD
user's functional description

USAMEDCOM
U.S. Army Medical Command

USANCA
U.S. Army Nuclear and Chemical Agency

USD (AT&L)
Under Secretary of Defense (Acquisition, Technology and Logistics)

USMTF
U.S. Message Text Format

V&V
verification and validation

VPG
virtual proving ground

VR
validation report

VV&A
verification, validation, and accreditation

WAN
wide area network

WIPT
working-level integrated product team

WRAP
Warfighting Rapid Acquisition Program